Intel® NetStructure™ 7190 Multi-Site Traffic Director

User Guide

intel

Intel® NetStructure™ 7190 Multi-Site Traffic Director v.3.1.1

User Guide

Technical Product Notice

Intel Corporation
Network Equipment Division
13280 Evening Creek Drive
San Diego, California 92128-4102
USA
Main: (858) 391-1900
Fax: (858) 391-1920

A20163-002 **November 29, 2000**

Table of Contents

1 Introduction

What is an Intel® NetStructure™ 7190 Multi-Site Director?

The Intel® NetStructure™ 7190 Multi-Site Traffic Director is a global site balancer. It gathers your geographically dispersed data sites into multiple "virtual servers," thus giving you multifaceted, centralized control over widely distributed resources.

Performance

The 7190 looks at individual client requests and matches them up with the best of many geographically dispersed fulfillment sites using the selection method most appropriate to your specific needs.

Reliability

The 7190 supports active-active redundant mode, meaning that multiple, active 7190s can be used simultaneously. When one fails, any remaining 7190s continue operation.

Scalability

The 7190 can work cooperatively with up to fifteen other 7190s in deployment across sites. A site may be managed by any Intel® NetStructure™ e-Commerce Traffic Director or Intel® NetStructure™ Commerce Director, which can in turn intelligently manage server farms, and return server performance data to the 7190. The 7190 also supports sites that do not have an Intel® load balancers.

Flexibility

The 7190 offers six distinct methods of balancing your distributed resources, ensuring a solution for your multi-site problems.

Two Versions of the 7190

There are two versions of the 7190. One uses strong encryption (128-bit encryption) and the other uses weak encryption (56-bit encryption). The 7190 version that may be exported to certain countries is subject to U.S. export restrictions.

Who Should Use This Book

This user guide is intended for network administrators with a basic knowledge of:

- Networking concepts and terminology
- Network topologies
- IP routing
- DNS and BIND

User Guide Summary

In addition to this introduction, the user guide contains the following chapters:

- **7190 Theory of Operation**
  An overview of the multi-site network, the 7190's place in it, and some concepts you need to know to use the unit effectively

- **CLI Configuration**
  Instructions on how to use the Command Line Interface (CLI) to manually configure additional sites, agents, zones, and services.
- **Multi-Site Scenarios**
  Descriptions of several typical multi-site challenges accompanied by their corresponding 7190 solutions
- **Boot Monitor**
  An explanation and reference of the 7190's configuration commands
- **CLI Reference**
  Detailed descriptions of the 7190's operational commands, including tree illustrations of the command system structure
- **SNMP Support**
  Details of 7190's SNMP capabilities
- **Software Updates**
  Software update procedures
- **Diagnostics (Appendix A)**
  How to interpret the 7190's LED display
- **Cleaning the Dust Filter (Appendix B)**
- **Regulatory Information (Appendix C)**
- **Terms and Conditions (Appendix D)**
  End user terms, conditions, and licensing information
- **Glossary**
- **Support Services**
- **Index**

Notes

2 Theory of Operations

NOTE: *Intel Load Balancer refers to either Intel®NetStructure™ 7180/7185 e-Commerce Directors or the Intel®NetStructure™ 7140/7145/7170/7175 Traffic Directors.*

Typical load balancers work by balancing traffic over a Local Area Network (LAN) to a Web farm. The Intel® NetStructure™ 7190 Multi-Site Traffic Director extends this balancing to multiple sites over a Wide Area Network (WAN). By balancing referrals to each site, the 7190 enables enterprises and Web hosting services to integrate geographically distributed content and services.

The advantages of such integration are many, including:

- There is increased fault tolerance and availability owing to redundant sites. Multiple active sites permit uninterrupted service in the event of a localized outage in the data network.
- Customer response times are improved by directing users to uncongested sites or data centers.
- Easy scaling of server farms can be accomplished.

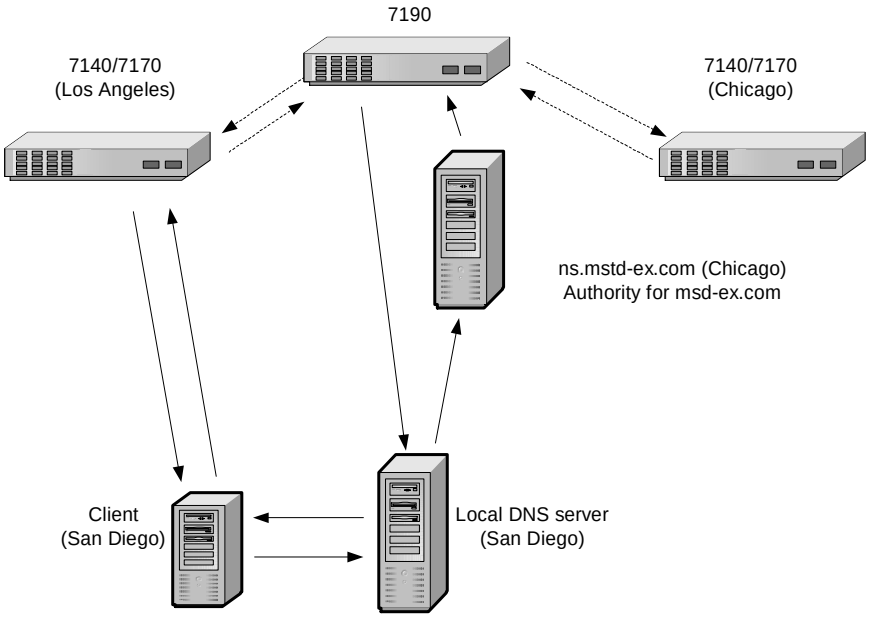
Multi-site load balancing works best in concert with Intel® load balancers. The 7190 also supports multi-site load balancing with sites that do not have Intel load balancers. In this case, the sites are balanced on the basis of availability, and not based on proprietary metric information.

"Intelligent" DNS

The 7190 leverages the DNS architecture and protocol as the basis for its site balancing operations. Based on the information gathered from all sites, the 7190 returns the address of the site that best meets the criteria for fulfilling the request.

Traditional DNS

Traditional, or Round Robin, Domain Name Service (DNS) is a rudimentary means of server load balancing. Under this method, a single hostname is mapped to a list of multiple server IP addresses. When the DNS server resolves a request for that hostname, it returns the entire list to the requestor, then sorts it (the first name drops to the end of the list). Upon receiving the list, the client requestor typically uses the first address. The next requestor of the hostname receives the resorted list, and again most likely uses the current first name. The list is resorted again, so that each sequential request sees a different "first choice" than the previous one. The chief benefit of Round Robin DNS is that it allows requests to be distributed to multiple hosts and, in theory, provides a layer of redundancy. On the negative side, the DNS server has no knowledge of the status of the sites to which it sends requests. Receiving sites may be heavily loaded or dead, thus the potential is high for unacceptably slow replies error messages to clients, which is out of the site operator's control.



Multi-Site Load Balancing

Authoritative DNS Servers

The DNS maps, or “resolves” hostnames into IP addresses. It is, in effect, a distributed database operating through a distributed, hierarchical system of Domain Name Servers. Thus, if the local DNS server cannot resolve a name, it looks “upstream” to consult a Root Domain Server for help. The Root Domain Server in turn asks the Authoritative Name Server (i.e., the owner of the name it is trying to resolve) to return the appropriate IP address for the requested name.

To illustrate

1. The client sends a query to its configured DNS (all clients are configured with the address of their DNS server) to resolve a particular domain name (e.g., *www.mstd-ex.com*).
2. The client DNS server sends a query to the Root Domain server for the .com domain (every DNS server is configured with the root server information) to resolve *mstd-ex.com*.
3. The Root Domain server responds with the address of the Authoritative DNS server for the *mstd-ex.com* domain.

4. The client DNS server sends a query to the *mstd-ex.com* Authoritative DNS server to resolve *www.mstd-ex.com*.
5. The Authoritative DNS server responds to the client DNS server with the IP address of *www.mstd-ex.com*.
6. The client DNS server responds to the client with the IP address of *www.mstd-ex.com.*

In the discussion above, the 7190 acts as authoritative DNS server for *zone.mstd-ex.com,* which is the zone in which the name *www.mstd-ex.com* resides.

Multi-Site Traffic Management Using Intel Load Balancers

Multi-site load balancing solves most of the problems inherent in Round Robin DNS. Under the server load balancing model, servers are aggregated in a "server farm" behind a load balancer known by a Virtual IP address or "service." (The service is the IP address of which the external network is aware.) By keeping track of such metrics as number of connections, which services are running, response time and the like, the load balancer knows the status of the servers. The 7190 retrieves metrics from the load balancer. Thus, when a client requests the service, the 7190 routes it to the site who has a server best able to fulfill it.

If the data center has an Intel Load Balancer, the 7190 works in concert with the "agents" in the load balancers by continually communicating with each site's agent through site verification protocol. This keeps the 7190 informed of the following:

- Health of the load balancers.
- Individual service health and availability.
- CPU utilization of load balancers (as of 7140/7170, 7180 Software release 2.2.1)
- Response time for each service (as of 7140/7170, and 7180 software release 2.3)
- Number of connections to each load balancers (as of 7140/7170, and 7180 software release 2.2.1)

Site verification protocol information is encrypted for secure communication between an Intel Load Balancer and the 7190.

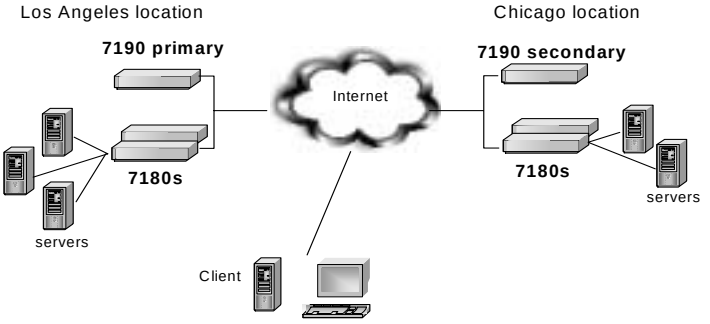
Multi-Site Traffic Management Without NetStructure Load Balancers

The 7190 can support data centers, whether or not they have an Intel Load Balancer. Without these Intel products, the 7190 can monitor site service availability by using an ISV method:

- Ping (ICMP)
- TCP Open probe
- HTTP URL probe

Typical Configuration

The 7190 can be used with a wide variety of topologies but a basic example of a 7190 configuration might consist of two 7190s and four NetStructure 7140s (one 7190 at each location that the site is distributed across, and two 7140s in serial fail-over mode for each location). For illustrative purposes, these devices are configured to balance *www.mstd-ex.com*. Because the 7190 does not resolve records aside from hostnames (e.g., no MX records or reverse DNS lookups), your existing DNS server should remain authoritative for the domain, *mstd-ex.com*. A new zone, *zone.mstd-ex.com*, must be created and your existing DNS server must delegate authority for this zone to all of the 7190s. An alias, www.zone.mstd-ex.com is created for *www.mstd-ex.com*. This zone and alias are transparent to users connecting to your site. They still requests *www.mstd-ex.com* and are referred to the optimal site by the 7190.



7190 Overview - A Basic Configuration

Site Balancing Methods

The 7190 supports six site-balancing methods or algorithms. The operator chooses the method most appropriate to the deployment to optimize traffic volume, priority, resource availability, and the overall desired outcome.

Weighted Algorithms

- **Weighted Round Robin** - Two differences distinguish this method from traditional, or *round robin*, DNS. First, the 7190 is aware of the status of the sites it balances thus, unlike legacy Round Robin, it does not indiscriminately send requests to servers that have gone down or are otherwise unable to fulfill requests. Second, *weighted round robin* allows the operator to skew the loading among available site services on the basis of an assigned "weight." (Weight takes into account differences in capabilities of site services.) Weighting allows the operator to adjust loading on a percentage basis. For example, Site A is assigned a weight of 1, Site B, 2, and Site C, 7. Thus, Site A receives 10% of the traffic, Site B, 20% and Site C, 70%. This method can ensure the most efficient use of those sites with greater "horsepower," while preventing the overtaxing of less powerful ones.
- **Weighted Random** - The Weighted Random method is similar to Weighted Round Robin with the exception that requests are not fulfilled serially. IP addresses are resolved in a random fashion. The weighting is accomplished as above. The benefit of this algorithm is that it is more effective at normalizing, or leveling, load.

Metric Algorithms

Using DNS to balance multiple sites is more effective when the referrals are based upon knowledge of the actual loads on the servers. In addition, balancing effectiveness noticeably increased when back-to-back referrals to the same site were not made even if metrics indicated one site service was the best both times. The 7190 metric algorithms reflect both of those findings.

These balancing algorithms are not available for sites that do not have Intel load balancers:

- **Response Time** - The Response Time method directs requests to the site that has the fastest aggregate (i.e., across all servers) response time for the requested service. Likely users of this method are enterprises that have identified the efficient

fulfillment of a specific type or types of traffic as being crucial to their business goals. (Available with the 7140/7170, 7180 2.3 release.)

- **Least Connections** - The Least Connections method sends requests to the site with lowest number of connections. This method permits the most efficient management of requests that are likely to require connections of long duration, such as FTP. (Available with the 7140/7170 and 7180 releases.)
- **CPU Utilization of Local Load Balancer** - This method directs clients to the site whose load balancer has the lightest workload. The benefit of this method is most evident when used with sites performing processor-intensive Layer 7 load balancing. (Available with the 7170 2.2.1 release.)

Managing Unequal Site Servers

There is a "factor" command to determine a threshold factor in the event of two unequal servers. (see **config dns zones** <zonename> **hostnames** <hostname> **siteservices** <siteservicename> **factor** in Chapter 5, "CLI Reference.")

The 7190 determines which IP address to return for a hostname, based on the performance of the IP address and port at a site. The three-step process is:

1. Determine the metric(s) with the smallest value.
2. Determine whether any remaining service(s) are close enough to this best value to also be considered. The quantification of "close enough" is the **factor**. A factor of 0 means consider only services with the best value.
3. Randomly choose from all the services identified in the first two steps.

A good example of the usefulness of this "close enough" threshold factor is when two unequal servers are deployed behind different load balancers. Server A may be capable of handling 3000 connections per second. Server B may also be capable of handling that many connections per second, but is also serving more sites than Server A. The realistic connection limit of Server B may therefore only be about 500 connections per second. If Server A has 900 connections and Server B has 400 connections, then Server B is the site with the least number of connections, although it is already 80% loaded while Server A is only 30% loaded. The better choice would be to give the traffic to server A. However, the 7190 has no knowledge of the actual

load potential of the servers underneath the load balancers it monitors. Therefore it allows the next best thing. For example, it allows the user to declare that if Server A is within 2400 connections (80% of maximum) of Server B, consider referrals to Server A even if Server B is the lowest. The factor setting would be 2400 for the service associated with Server A and 0 for the service associated with Server B.

Flash DNS

Network topology can greatly affect the overall transfer rate between a site and a client. A solution is to replicate sites on multiple networks (which are sometimes also distributed geographically). Without a 7190, it can be cumbersome to provide users with a list of mirror sites and then let them choose which one appears to be best for them.

Flash DNS addresses this problem by letting a 7190 at each network site send out responses to a DNS query for the site host name. If all responses are sent at the same time then the site that has the least network latency connecting to the user should get its response to the user first. The user ignores all the other responses.

Since many enterprise clients are behind firewalls that perform Network Address Translation (NAT), by default, the 7190 performs source IP using the IP address of the 7190 that originally received the DNS request. This feature can be disabled.

Partial Failures

The 7190 maintains the current metric state of each service on a per host basis. A “service” is an IP address and port at a site. The maintained state has four levels relating to the amount of information that the 7190 has about each service.

Each load balancing method handles partial failures in the same basic way. Each balancing method always tries to find at least one service with a metric status of “OK” with which to balance. If no services are available at this highest metric state, and it is not using a metric balancing method, then it looks for at least one service with a metric state of “No Services”. If none are found then it looks for at least one service with a metric state of “No Metrics”. Finally, if no services have been found at a high enough metric state level to balance normally, it performs a round robin selection among all the enabled services.

Status: OK

This state indicates that the required services behind this service are available on the associated load balancer. The metrics information for this service are current and can be used for metric load balancing.

Status: No Services

This state indicates that services other than the one(s) configured as required for the associated host are not available on the load balancer. Other services with this same service are available. Metric load balancing is not available for this service.

Status: No Metrics

This state indicates that the Intel Load Balancer is not advertising any services that use this service. Metric load balancing is not available for this service.

Status: No Connection

The 7190 has lost or been unable to establish a connection to the fulfillment agent on the load balancer. No metrics information on any services from this load balancer is available. No load balancing methods are available for this service. It may only participate in non-weighted round robin load balancing.

Service Standby

To achieve site service redundancy, customers often want to have backup services that are completely dark to normal traffic, but are instantly available to take over for a failed site service. The transition of traffic from the failed site service to the standby site service occurs without the need of operator intervention.

The Service Standby feature allows the designation of a site's services for standby. If there is a 7190 located at the site, its operation is unaffected and continues in resolving queries and referring to active services. When the 7190 has detected a failed service, the failed service is not used in referrals. Once a failed service has been deemed active again, no further referrals are made to the standby service.

The determination to use or not use a standby site service is only made upon receipt of a query that involves the service. Therefore, a standby service is not activated to replace a failed service until a query is received, and a failed service is not shown as active until after a query is received.

Multiple VIP Response

The DNS response from a 7190 may contain multiple answers. The number of answers and whether to include stand-by VIPs can be configured.

Active VIPs are included first in the response. A stand-by VIP is treated as an active VIP, if it is marked as "IN USE" due to a failed VIP. Stand-by VIPs are included after the active VIPs: (a) if the configuration is set to include them and, (b) the number of requested additional VIPs in the response has not been met.[1]

When using mutli-VIP response with Flash load balancing, the Flash response attempts to use VIPs within the same peer group first before including VIPs from the other peer groups.

Definitions

Understanding of the 7190 requires some specialized terms. The definitions provided here are specific to the context of multi-site load balancing and the operation of the 7190, thus there may be subtle differences between these and those offered in other sources.

Agent is a component of an Intel Load Balancer that gathers metric data and transmits it to the 7190. For the purposes of the discussions in this user guide, "agent" is synonymous with "Traffic Director" or "e-Commerce Director."

Agent IP refers to the real IP address of an Intel Load Balancer in its role as an agent to a 7190.

Intelligent Site Verification (ISV) is used to directly determine the availability of (1) a service or, (2) a service that is balanced using a third-party Load Balancer. Methods of verification include a site ping, TCP connect, and HTTP probe.

ISV Group refers to a collection of services available at a physical site. All services in a group share the same ISV polling parameters.

---

1. If multi-VIP standby is enabled when using the Flash load balancing method, standby VIPs from a site are not included if all of the VIPS are (1) standby and, (2) not marked "IN USE" due to a failed VIP at another site.

Primary 7190 is a 7190 that automatically transfers (copies) configuration information to secondary 7190s (through the Global Sync process). Configuration may only be changed on a Primary 7190.

Service is the Virtual IP (VIP) and port number of an application service available at a site.

Authoritative Server is a DNS name server that has complete name space information regarding the hosts within a given *zone* (see below).

Authority is an attribute of a DNS name server with respect to a specific part of the DNS name space, or zone (see below). A name server is said to have authority over a zone, by which that server has complete name space information for that zone.

Zone is a portion of a DNS name space for which a given name server has complete name space information. When a name server receives a request for a host outside of its zone, it replies with the name of the name server that is authoritative for a different zone and is likely to have the specific information required to satisfy the request.

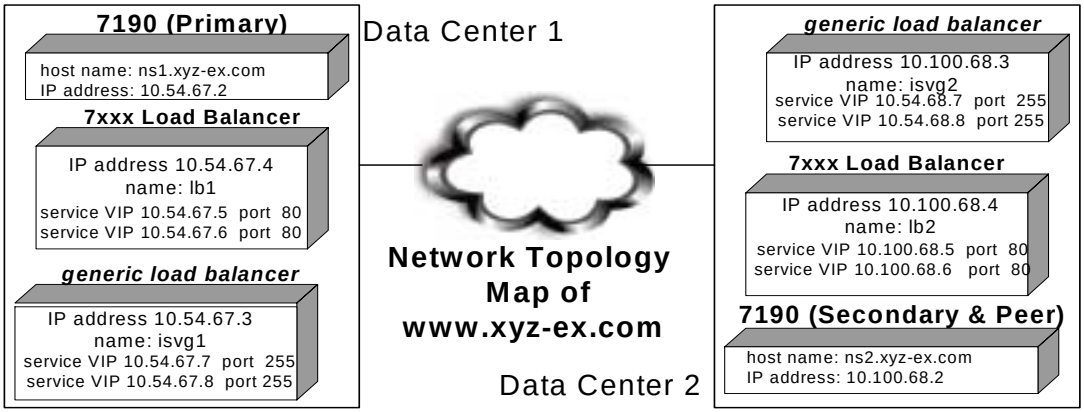
Notes

3 CLI Configuration

Custom/Manual Configuration

You can manually change any specific configuration parameters if any of the Quick Start Wizard default settings are not sufficient for your site.

It is recommended that you use the custom configuration method only after you have completed the initial configuration with the Quick Start Wizard. See the *Intel® NetStructure™ 7190 Multi-Site Traffic Director Getting Started Guide* for instructions on using the Quick Start Wizard.



Sample Network Topology

Adding Secondary 7190(s)

Now that the primary 7190 is up and running, the additional 7190s can be easily added by configuring them as secondary 7190s. They receive all their configuration information from the designated primary 7190 through the Global Sync process, which automatically transfers the primary 7190 configuration to any secondary 7190s.

Similar to a typical DNS server, all 7190s are treated as equals by other DNS servers. The terms of primary and secondary only refers to where a 7190 gets its new configuration information. The 7190 only allows the configuration to be changed on a primary 7190. Secondaries get their configuration from their designated primary 7190 and store a copy of the received configuration locally. Should a secondary be unable to contact a primary it functions normally using its stored configuration. All 7190s have the same picture of the current Agent metrics and are equally capable of responding. Should one fail the existing DNS protocol automatically routes requests to the non-failed 7190s.

The theoretical secondary *ns2.xyz-ex.com* (IP 10.100.68.2) can resolve requests for *www.somedomain.xyz-ex.com* by becoming a secondary of the 7190 at 10.54.67.2. From the CLI on the proposed second 7190, execute the command:

NOTE: User-entered names and IP addresses in the example are for illustrative purposes only. The appropriate values for your installation may vary.

```
#config dns secondary 10.54.67.2
Warning: Your current dns configurations will
be lost.
Are you sure you want to become a Secondary
(Yes/No):yes
Now running as a Secondary.
```

If the DNS configuration of 10.54.67.2 is changed, the new configuration can be propagated to 10.100.68.2 by the **`commit all`** command.

Creating Agents

An Intel_7xxx Load Balancer refers to Intel®NetStructure™ 7180/7185 e-Commerce Directors or the Intel®NetStructure™ 7140/7145/7170/7175 Traffic Directors.

An agent refers to the Intel Load Balancers at each site. They are used to keep the 7190 informed of site status, response time, and number of current connections of the server farm they are balancing.

To add an agent, type the following:

```
Intel 7190# config dns agents create lb1 ip
10.54.67.4
Intel 7190# config dns agents create lb2 ip
10.100.68.4
```

Associating Services with Agents

Next, services must be associated with agent(s):

```
Intel 7190# config dns agents lb1 services
create 10.54.67.5:80
Intel 7190# config dns agents lbi services
create 10.54.67.6:80
Intel 7190# config dns agents lb2 services
create 10.100.68.5:80
Intel 7190# config dns agents lb2 services
create 10.100.68.6:80
```

Creating Zones

The next step is to create a zone (e.g., *somedomain.xyz-ex.com*) on the 7190. The command to do this is:

```
Intel 7190# config dns zones create
somedomain.xyz-ex.com
```

NOTE: *The 7190 must be authoritative for this zone—the existing DNS server should delegate the domain to the 7190.*

Creating Authority Records

Next, authority records for your two 7190s are created. These sites are used to tell DNS servers who they can query directly for other hosts in the current zone. In order for the 7190 to perform effectively, only 7190s should be authoritative for the zone.

For example, hostname *ns1.xyz-ex.com* at IP address 10.54.67.2 and hostname *ns2.xyz-ex.com* at 10.100.68.2. The authoritative DNS servers for *xyz-ex.com* should contain records for these hostnames, as well as the corresponding NS records for *somedomain.xyz-ex.com.* (See the section, *Existing DNS Servers*.)

```
Intel 7190# config dns zones somedomain.xyz-ex.com

7190/config/dns/zones/somedomain.xyz-ex.com# create-authority ns1.xyz-ex.com ip 10.54.67.2

Create Authority Successful

7190/config/dns/zones/somedomain.xyz-ex.com# create-authority ns2.xyz-ex.com ip 10.100.68.2

Create Authority Successful

7190/config/dns/zones/somedomain.xyz-ex.com# info

Zone: somedomainex.xyz-ex.com

   Authority Records TTL: 7200

   Authority Name: ns1.xyz-ex.com
   Authority IP:   10.54.67.2

   Authority Name: ns2.xyz-ex.com
   Authority IP:   10.100.68.2

Zone = somedomainex.xyz-ex.com

Authority Records TTL = 7200

Authority Name : ns1.xyz-ex.com

Authority IP: 10.54.67.2

Authority Name : ns2.xyz-ex.com

Authority IP: 10.100.68.2
```

Creating Hosts

Next, the hostname *www.somedomain.xyz-ex.com* is created:

```
7190/config/dns/zones/somedomainex.xyz-
ex.com# hostnames create www

Create Hostname Successful
```

The next step is to map the services *www.somedomain.xyz-ex.com to* the load balancer. The following assumes the IP addresses of the load balancer to be 10.54.67.4 (service 10.54.67.5:80) and 10.100.68.4 (service 10.100.68.5:80), and that the agents are enabled and running on the default port 1999. (Agents are enabled or disabled using the CLI of an Intel Load Balancer, with the command, `config sys multisite <enable|disable>`.) It is assumed that the agent names are the same as their IP addresses.

```
7190/config/dns/zones/somedomainex.xyz-
ex.com# hostnames www siteservices

7190/config/dns/zones/somedomainex.xyz-
ex.com/hostnames/www/siteservices# map
lb1:10.54.67.5:80

Site Service Mapped

7190/config/dns/zones/somedomainex.xyz-
ex.com/hostnames/www/vips# map
lb2:100.68.5:80

Site Service Mapped
```

Commit the Configuration

The **`commit`** command is used at this to point put the configuration into effect.

```
7190/config/dns/zones/somedomain.xyz-ex.com/
hostnames/www/vips# commit all

Warning: Your active configuration will be
overwritten.

Are you sure you want to commit the
configuration (yes|no)? yes

Configuration has been committed
```

NSLookup

The nslookup utility can verify that the 7190 is correctly resolving *www.somedomain.xyz-ex.com*:

```
Intel 7190# nslookup
www.somedomain.xyz-ex.com
Server: server1.xyz-ex.com
Address:192.168.16.4
Name:    www.somedomain.xyz-ex.com
Address: 192.168.16.23
```

Configure DNS Servers

The existing DNS server or servers must be correctly configured to work with the 7190s. Entries need to be made that delegate the responsibility of resolving DNS queries for www.xyz-ex.com to the 7190s. This can be done in one of two ways. The first way is to delegate the entire zone to the 7190. This works fine as long as only type A records need to be returned for this zone. The 7190 is a high performance specialized DNS server and supports only the more common type A records.

NOTE: *If the 7190 was not configured with a primary name server during setup from the Boot Monitor, the* ***nslookup*** *command fails.*

The recommended way of configuring your existing DNS server is delegate partial authority by aliasing. All of the 7190s (both primary and all secondaries) must be included in the authority record (NS) portion of the delegation.

Multiple-VIP Response

A DNS response may contain multiple answers. A standby VIP is automatically considered as a response if it is marked "IN USE" due to a failed VIP. When multi-VIP standby is enabled, standby VIPs are included in a response if the number of additional VIPs in the response has not been met[2]. To include standby VIPs, type `config dns zones <zonename> hostnames <hostname> multi-vip-standby enable`.

```
7190#config dns zones somedomain.xyz-ex.com
hostnames www multi-vip-standby enable
```

[2] If multi-VIP standby is enabled when using the Flash load balancing method, standby VIPs from a site are not included if all of the VIPS are (1) standby and, (2) not marked "IN USE" due to a failed VIP at another site.

The number of additional answers in a response can be configured. The range is from 0 to 15.

```
7190#config dns zones somedomain.xyz-ex.com
hostnames www add-rec-responses 4
```

To verify whether multi-VIP standby is enabled or check the number of additional responses, type `config dns zones <zonename> hostnames <hostname> info`.

```
7190#config dns zones somedomain.xyz-ex.com
hostnames www info
```

Notes

4 Multi-Site Scenarios

Scenario 1

One Web site, two geographical sites (one server each), two 7190s, optional 7110s

Introduction

An e-commerce company with a single Web site (www.mstd-ex.com) wants to expand their site to two geographically dispersed locations so that customers can be referred to the site that gives them the fastest response time. They initially deploy only a single server at each site (no load balancers), but they want the ability to expand as the demand on their Web site increases.

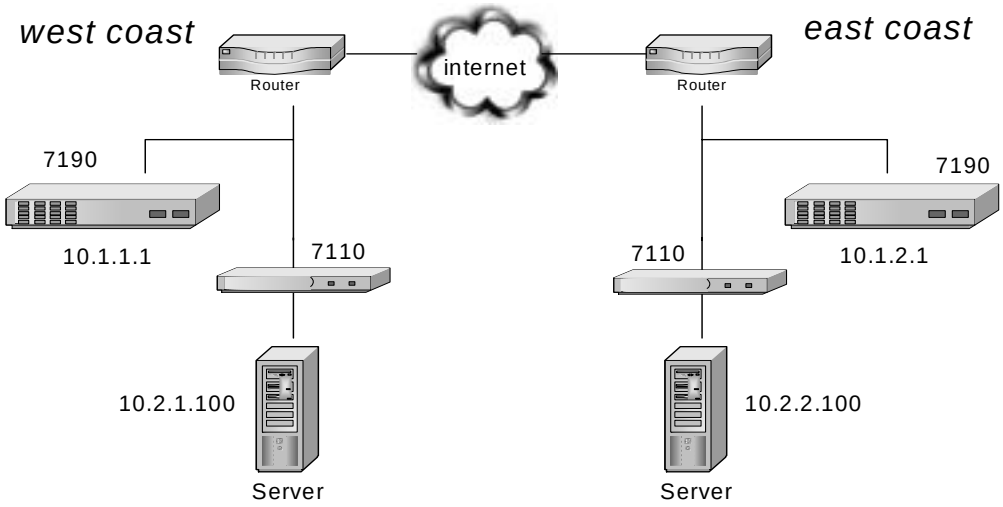
Initially, a 7190 would be deployed at each site. Optional 7110s could be deployed in front of each server for HTTPS traffic. Since only one server is being deployed at each site no load balancers are required. The 7190s is set up to monitor the health of the Web site by performing a periodic HTTP probe of the main Web page on each server. After verification that the initial configuration is working properly, the balancing method is

changed to Flash Response Mode to deliver the site that has the least network latency to potential customers.

Part 1 – Initial Configuration of a Simple Site

Key Concepts:

- No Load Balancers (non-brokered)
- ISV
- Two Sites
- Configuring a Secondary 7190
- Delegating Authority to a 7190



Simple Site (Scenario 1)

Procedure

In this scenario each site is treated as its own ISV Group, since there are no load balancers at either site. Both sites could be put into one single ISV Group for this simple example, but for a majority of situations it is better to have a one-to-one mapping of ISV Groups to sites.

The 7190 at the westcoastsite is the primary 7190. Except in very rare cases there should only be one primary 7190. All other 7190s in the network should be secondaries so they can slave their configurations to the primary 7190.

Step 1. Create the ISV Groups for each site and associate their services.

The creation of an ISV Group is primarily for management purposes. The ISV Group is referred to by name. This allows you to choose a name that is meaningful to you in your network environment (e.g., westcoastsite). Names are case insensitive.

```
config dns isvgroups
create westcoastsite
westcoastsite services create 10.2.1.100:80
create eastcoastsite
eastcoastsite services create 10.2.2.100:80
info
```

Step 2. Select HTTP probe as the ISV method and associate a URL with each service.

Since there are no load balancers, ISV must be used to determine site service availability. In this scenario the site represents a distributed Web site. The best way of determining site service availability is a combination of ISV and traffic monitoring. Only a load balancer can do this. The next best thing is ISV using an HTTP probe. For this scenario only the main Web page (http://www.mstd-ex.com/main.html) is probed.

NOTE: *Only the actual file name is entered in the URL string. The Service VIP and Port already imply http://www.mstd-ex.com.*

```
config dns isvgroups westcoastsite services
10.2.1.100:80
url /main.html
config dns isvgroups eastcoastsite services
10.2.2.100:80
url /main.html
```

Step 3. Create the delegated zone for the hostname and the authority records for the zone.

In order for the rest of the world to know that the 7190s are the place to go for resolving the hostname www.mstd-ex.com they must be made authoritative for the domain mstd-ex.com. This could be

impractical, so the solution is to make the 7190s authoritative for a zone within the mstd-ex.com domain, rather than for the entire domain. For this example the authoritative name server for the mstd-ex.com domain delegates authority of a new zone within its domain to the 7190. This zone is called geo.mstd-ex.com. The hostname www.mstd-ex.com is aliased to www.geo.mstd-ex.com. Anyone querying the mstd-ex.com name server for the address of www.mstd-ex.com is told to ask one of the 7190s for the address of www.geo.mstd-ex.com.

```
config dns zones

create geo.mstd-ex.com

geo.mstd-ex.com create-authority nswc.mstd-
ex.com ip 10.1.1.1

geo.mstd-ex.com create-authority nsec.mstd-
ex.com ip 10.1.2.1

info
```

Step 4. Create Host and Specify Balancing Method.

When you create the hostname you can specify the balancing method to use in selecting which site services are referred. For this scenario, the balancing method eventually is Flash Response Mode. But for initial testing of the network and configuration it is often best to configure first with Weighted Round Robin mode. This allows for easy verification of the configuration because the query responses are deterministic. Once the initial configuration is verified the balancing method can be changed to the production method (*Part 2* of this scenario).

```
config dns zones geo.mstd-ex.com hostnames

create www

www method wrr

info
```

Step 5. Map Services to Hostname.

DNS is essentially a means of mapping hostnames to IP addresses. The 7190 takes this mapping one step further by allowing the mapping of hostnames to services (IP address and service port). In this step the services that were created in Step 1 are mapped to the hostname created in Step 2.

```
config dns zones geo.mstd-ex.com.
hostnames create www
www siteservices
map westcoastsite:10.2.1.100:80
map eastcoastsite:10.2.2.100:80
info
```

Step 6. Save and activate the configuration.

The 7190 maintains two copies of configuration. One is the active copy of the configuration used by the name server function of the 7190. This configuration is accessed by all the **show** commands. The other copy is for in-work changes of the configuration. This configuration is accessed by all the **config** commands. This is the copy in which we have been entering the new configuration. In order to make the current in-work configuration active, the configuration must be committed using the **commit** command.

Save and **Commit** commands: The difference between the **save** and **commit** commands is often a source of confusion for new users. The **save** command is used to make a snapshot of the active configuration. The **commit** command is used to make the in-work configuration active. Once you have a good working configuration it is always a good idea to save a snapshot of this configuration before you do your next commit. This way if there is a problem with the new configuration you can use the **restore** command to revert to the previous configuration.

```
commit all
```

Step 7. Configure the Secondary 7190.

Configuration of secondary 7190s is very easy. First you use the Boot Monitor to configure the hardware and network information (see the chapter on *Installation, Startup and Configuration*). Then you choose "Become a Secondary" in the Quick Start Wizard when it comes up. Enter the IP address of the primary 7190 (10.1.1.1). In a matter of seconds after issuing the command the secondary has a copy of the configuration from the primary. Subsequent **commit** commands automatically transfer the configuration to every attached secondary. This automatic process of transferring (copying) a configuration from primary to secondary 7190s is called Global Sync.

Step 8. Delegate authority to the 7190s.

The primary name sever responsible for the mstd-ex.com domain needs to be modified. The modifications vary depending on the type and version of the DNS server used. For this example it is assumed that a Bind server is being used.

At a Bind DNS server, add the following lines to the database file for the mstd-ex.com domain. Typically this file would be called something like "db.mstd-ex".

```
geo.mstd-ex.com.     IN NS    nswc.mstd-ex.com.

geo.mstd-ex.com.     IN NS    nsec.mstd-ex.com.

nswc.mstd-ex.com.    IN A     10.1.1.1

nsec.mstd-ex.com.    IN A     10.1.2.1

www.mstd-ex.com.     CNAME www.geo.mstd-ex.com.
```

Step 9. Verify the configuration and network operation.

There are many tools available to accomplish this step. The simplest is to ping www.mstd-ex.com. Since we have initially configured for Weighted Round Robin (with a weight of 1) we expect to ping 10.2.1.100. After waiting at least 60 seconds (the default Time To Live for a 7190 response) perform another ping. This time it should ping 10.2.2.100. Performing this a third time should result in the first service being pinged again.

Part 2 – Changing to Flash Response Mode Balancing

Key Concepts:

- Flash Response Mode
- Associating 7190s with a site

Procedure

Now that the 7190 is configured and functioning properly it is time to modify the configuration to use Flash Response Mode balancing instead of Weighted Round Robin.

Step 1. Associate 7190s with a site.

Flash Response Mode works by sending DNS responses back to the client from a source that is as close (network wise) as possible to the address it is returning. Only the 7190s are capable of sending Flash responses.

```
config dns isvgroups westcoastsite
flash-src 10.1.1.1
config dns isvgroups eastcoastsite
flash-src 10.1.2.1
```

Step 2. Change the host balancing method to Flash Response Mode.

```
config dns zones geo.mstd-ex.com
hostnames www
method flash
```

Step 3. Commit the configuration changes.

Now that the changes are completed, save a snapshot and commit the configuration. Note that now that a secondary 7190 is online these configuration changes are instantly propagated to the secondary 7190 (eastcoastsite) whenever the **commit all** command is executed.

```
save first-cfg
commit all
```

Part 3 – Adding Load Balancers to an Existing Site

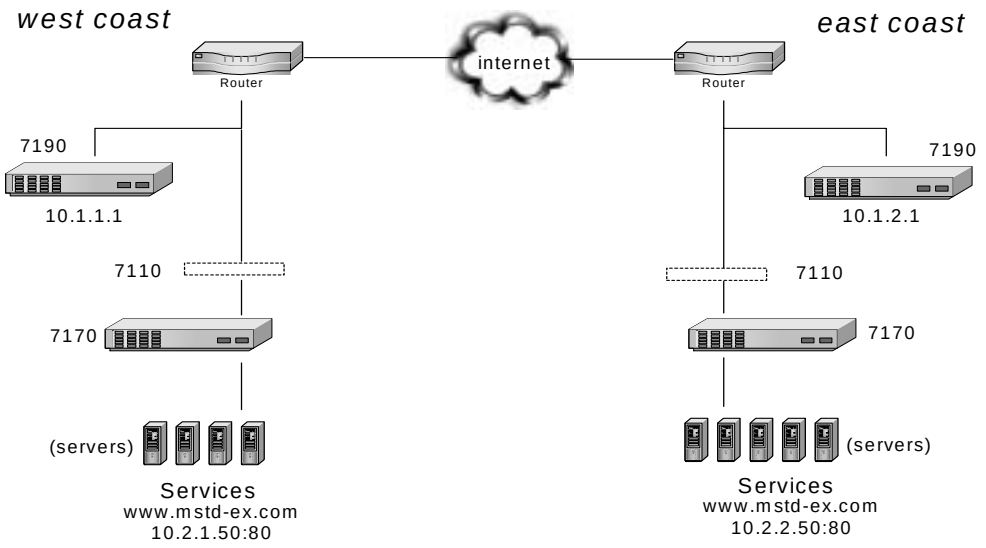
Key Concepts:

- Adding a Load Balancer (Agent)
- Disabling a Site
- Mixture of Brokered and Non-brokered Sites
- Configuring for Future Expansion
- Deleting an ISV Group
- Adding and Deleting Services

After the sites have been up and running for a while it is still easy to change the configuration to add new servers, services and hosts. But if the site data traffic increases significantly it is often advantageous to add load balancers to manage the traffic to the Web servers. Done correctly, the addition of a load balancer at a site can be handled with minimal service interruption.

There are two methods to handle this transition. The first method requires that all existing network addresses be kept in place. The 7190s would continue to refer clients directly to the servers until the configuration changes are committed. The second method assumes that addresses of the servers might change. The act of changing network addresses of servers usually entails taking a site offline while transitioning.

The 7190 has some built-in features that make this transition almost as simple as the first method. In this section, the 7190 is used to take sites offline (no new referrals) to add a load balancer at each site.



ISV Groups and Services

Step 1. Add the load balancers and their services to the 7190 configuration.

The 7190 allows agents (load balancers) and ISV Groups and their services to be added prior to their availability. They can be added and then designated as disabled. This prevents any referrals to the new services until they are enabled. When an agent or ISV Group is disabled all their services are automatically disabled in every hostname that currently uses them. Further, no communication is attempted to the disabled agent/ISV Group.

If a service is disabled individually, but the agent/ISV Group is left enabled then no referrals are made to that service, but communication is attempted to the services associated agent/ISV Group.

```
config dns agents
create westcoastbroker ip 10.1.1.2
westcoastbroker
services create 10.2.2.50:80
disable
config dns agents
create eastcoastbroker ip 10.1.2.2
eastcoastbroker
services create 10.2.2.50:80
disable
config dns agents info
```

Step 2. Map the new services to a hostname.

When services are mapped to a hostname they are set to the enable state of their parent agent/ISV Group. If the agent/ISV Group is disabled then the mapped service is disabled. In the last step we created agents and disabled them. Therefore we do not need to explicitly disable them after mapping them.

```
config dns zones geo.mstd-ex.com
hostnames www siteservices
map westcoastbroker:10.2.1.50:80
map eastcoastbroker:10.2.2.50:80
```

Step 3. Delete the first site to transition over.

For the purposes of this scenario, the eastcoastsite converts over first. By deleting the site (deleting the sites ISV Group), the 7190s makes all new referrals to the remaining sites. In this case that leaves just the westcoastsite, since the brokered sites are still disabled. Deleting a site also causes the removal of all of its associated services from hostname mappings. To prove this, check the hostname after deletion.

```
config dns isv-groups
delete eastcoastsite
config dns zones geo.mstd-ex.com hostnames www
info
```

Step 4. Commit the new configuration.

At this point, you can save and commit the configuration.

```
save before-upgrade
commit all
```

Step 5. Bring the new eastcoastbroker hardware on line.

After the commit, the site known as *eastcoastsite* no longer receives traffic from new referrals. It may still continue to receive some residual traffic from cached referrals or current connections. Configure the load balancer known as the *eastcoastbroker*. Verify that it has the service 10.2.2.50:80 configured.

Step 6. Enable the eastcoastbroker and delete the westcoastsite.

Similar to disabling an agent, enabling an agent automatically enables all of its services mapped to hostnames.

```
config dns agents eastcoastbroker enable
config dns isvgroups
delete westcoastsite
commit all
```

Step 7. Bring the new “westcoastbroker” hardware on line.

After the commit, the site known as “westcoastsite” no longer receives traffic from new referrals. It may still continue to receive some residual traffic from cached referrals or current connections. Configure the load balancer known as the “westcoastbroker”. Verify that it has the service 10.1.2.50:80 configured.

Step 8. Enable the westcoastbroker.

After this step both sites are operational, and talk to the load balancers.

```
config dns agents westcoastbroker enable
commit all
```

Scenario 2

Multiple sites, server farms, multiple hostnames, multiple 7190s, generic (not Intel) load balancer

A large company with multiple divisions wants to integrate most of those division Web sites onto server farms located at two new geographically dispersed data centers. One division already has an existing brokered server farm at a third site that they refuse to give up. The load balancer at this third site is not an Intel load balancer. They want all of the Web traffic to be balanced between all of these sites. The division with the legacy brokered site wants to direct clients to the site with the least network latency (Flash Response Mode). They are extremely concerned about site availability and do not tolerate a solution that has any single point of failure. To further minimize the impact of any network outages that may affect one of their sites, they are establishing a smaller backup site that is used for testing new pages and should only receive traffic if one of the main sites fails. Because each division of the company is maintaining its own Web sites on the servers, multiple hostnames with different services for each hostname must be supported. The types of services vary from HTTP, HTTPS to FTP.

This scenario is meant to emphasize the flexibility of the 7190 for handling a wide variety of diverse requirements simultaneously. *Scenario 1* concentrated on basic configuration issues. *Scenario 2* concentrates on features not previously mentioned (redundancy and service standby) as well as the advantages of using the 7190 with Intel load balancers (metric load balancing).

Configuring in a Mixed Environment

Key Concepts:

- Redundancy
- Service Standby
- Four (4) Sites
- ISV
- Generic (not Intel) Load Balancers
- Metric Load Balancing
- Flash Response Mode
- Mixture of Brokered and Non-brokered Sites

- Different Site Combinations for Each Hostname
- Different Balancing Methods for Each Hostname
- Associating Services with Hostnames

Procedure

Step 1. Create agents for each of the sites brokered by Intel load balancers and associate their services.

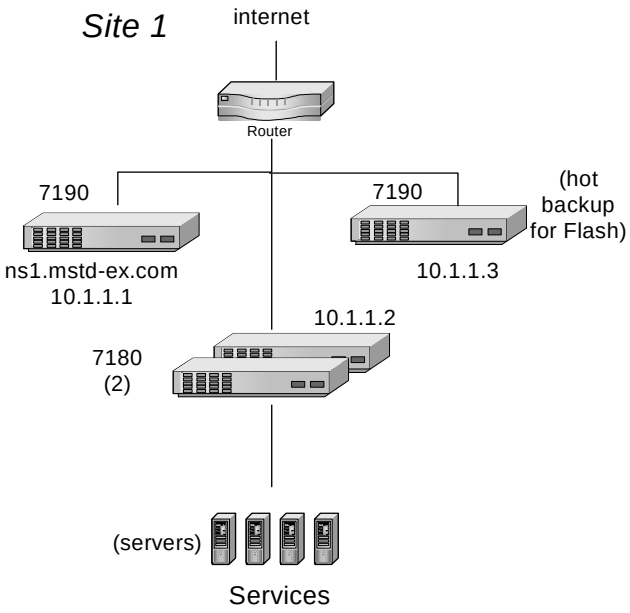
For this example, there is one existing site used for only one division's Web site. This site enforces the fact that not all sites have to be identical.

The 7190-to-site association is also done at this time since at least one Web site uses Flash Response Mode. The load balancers are used as the backup Flash source. In this scenario of four sites only two 7190s are actually required. If Flash Response Mode is used the load balancers can broadcast the DNS responses under the direction of the 7190s, but using the load balancers may have an impact on performance, so it is recommended that a 7190 be placed at each site and the site load balancer designated as a backup Flash source. This prevents the 7190 from being a single point source of failure without impacting the performance of the load balancer except upon a 7190 failure.

Since redundancy is a key issue, all of the load balancers are deployed in pairs with serial failover enabled. This means that each load balancer actually has three IP addresses. The IP address that is used to communicate with the 7190 is the Online Outside IP Address (management address). This makes the failure of a load balancer transparent to the 7190 except for a momentary loss of connection that provides the load balancer metrics.

- Create Site 1 and associate services:

```
config dns agents
create site1 ip 10.1.1.2
site1
flash-src 10.1.1.1
flash-backup-src 10.1.1.3
services
create 10.1.1.100:80
create 10.1.1.100:443
create 10.1.1.102:21
create 10.1.1.103:80
```

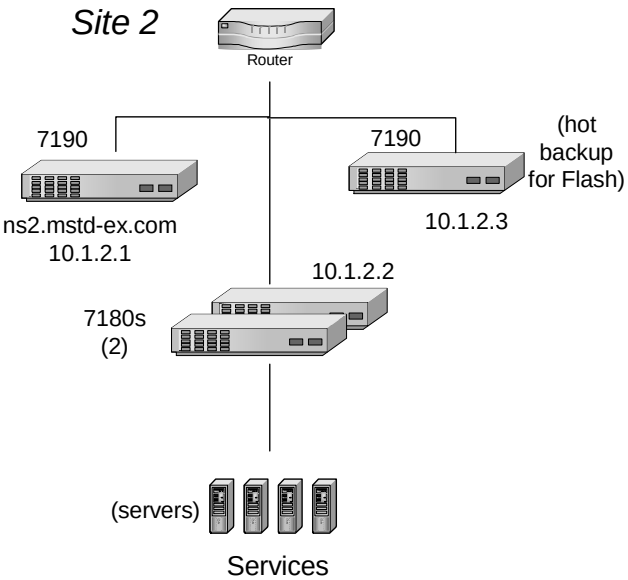


www.mstd-ex.com 10.1.1.100:80
www.secure.div1.mstd-ex.com 10.1.1.101:443
ftp.div1.mstd-ex.com 10.1.1.102:21
www.div2.mstd-ex.com 10.1.1.103:80

Site 1

- Create Site 2 and associate services:

```
config dns agents
create site2 ip 10.1.2.2
site2
flash-src 10.1.2.1
flash-backup-src 10.1.2.3
services
create 10.1.2.100:80
create 10.1.2.100:443
create 10.1.2.102:21
create 10.1.2.103:80
```

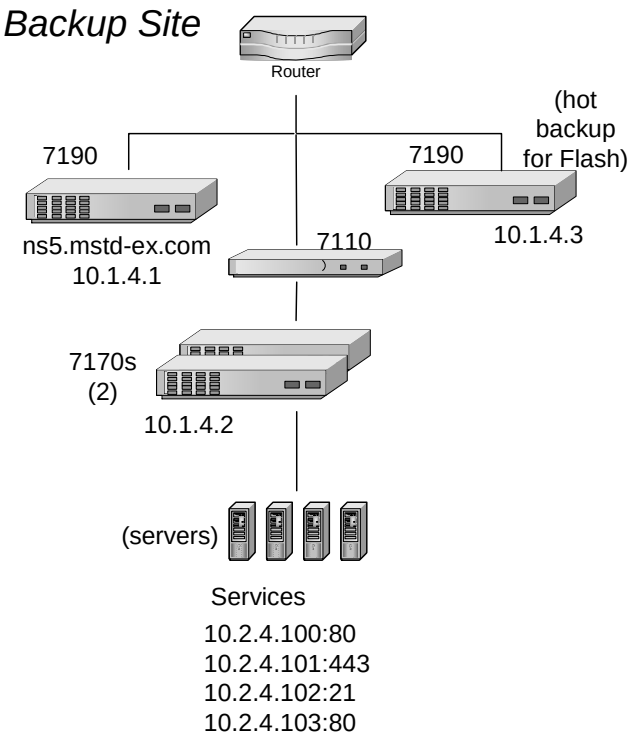


www.mstd-ex.com 10.1.2.100:80
www.secure.div1.mstd-ex.com 10.1.2.101:443
ftp.div1.mstd-ex.com 10.1.2.102:21
www.div2.mstd-ex.com 10.1.2.103:80

Site 2

- Create Backup Site and associate services

```
config dns agents
create backupsite ip 10.1.4.2
backupsite
flash-src 10.1.4.1
flash-backup-src 10.1.4.3
services
create 10.2.4.100:80
create 10.2.4.100:443
create 10.2.4.102:21
create 10.2.4.103:80
```



Backup Site

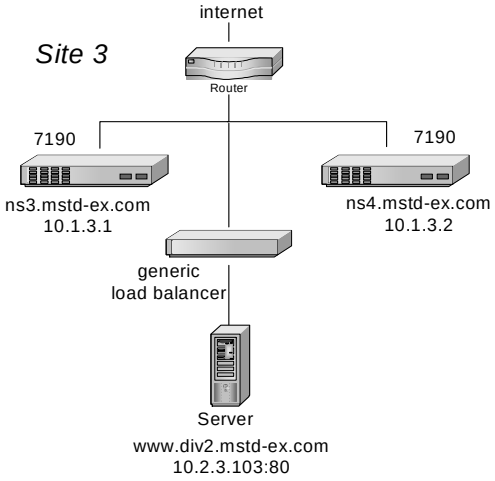
Step 2. Create ISV Group for the generic (not Intel) brokered site and associate its service.

This site is a legacy site with a generic load balancer. The 7190 can function quite well in this environment, but is not able to obtain metric information to support one of the metrics oriented balancing methods. Generic load balancers should be set up as an ISV Group. The brokered services offered by the load balancer are configured in the 7190 just like any other service (VIP and port).

Assume that the Web pages behind the single HTTP service available at the site are constantly changing. In this case it might be unwise to probe for a specific URL, and preferable to verify the presence of the HTTP server by attempting a periodic TCP connection.

The scenario description stated that the service provided at this site was to use Flash Response Mode. Since no load balancer is present, only the 7190 can broadcast Flash responses. This is a single point of failure, so a second 7190 is located at this site. The second 7190 does not need to be listed as authoritative for any zones, but this would be a waste of a good resource.

```
config dns isv-groups
create site3
site3
flash-src 10.1.3.1
flash-backup-src 10.1.3.2
services
create 10.2.3.103:80
10.2.3.103:80 method tcp
```



Site 3

Step 3. Create the delegated zones for the hostnames and the authority records for each zone.

Since 7190s are deployed at every site there is no reason to not utilize all of them to their full capabilities. All that is required to do this is to make all of the 7190s authoritative for both zones. Note that there is no need for the ns3 and ns4 to be listed as authoritative in the div1.mstd-ex.com zone. Further note that the 7190s used for hot standby redundancy are not listed as authorities. If it were not for the requirement of using Flash Response Mode for balancing www.div2.mstd-ex.com, there would need to be only two 7190s in the entire network. A 7190 only needs to be collocated (on the same network) with a site if Flash Response Mode is used and the load balancers are not configured as a primary Flash source for performance reasons.

```
config dns zones
create div1.mstd-ex.com
div1.mstd-ex.com
create-authority ns1.mstd-ex.com ip 10.1.1.1
create-authority ns2.mstd-ex.com ip 10.1.1.2
create-authority ns3.mstd-ex.com ip 10.1.1.3
create-authority ns4.mstd-ex.com ip 10.1.1.4
```

```
create-authority ns5.mstd-ex.com ip 10.1.1.5
config dns zones
create div2.mstd-ex.com
div2.mstd-ex.com
create-authority ns1.mstd-ex.com ip 10.1.1.1
create-authority ns2.mstd-ex.com ip 10.1.1.2
create-authority ns3.mstd-ex.com ip 10.1.1.3
create-authority ns4.mstd-ex.com ip 10.1.1.4
create-authority ns5.mstd-ex.com ip 10.1.1.5
```

Step 4. Add hosts for the first zone and map their services.

A limitation of DNS is there is no built-in way of conveying exactly what service the client actually needs. A request for *www.mstd-ex.com* could easily be for either HTTP or HTTPS service. A major feature of the 7190 is that it is service aware. It knows about the actual availability of services and can direct clients to the best site for that service. The problem lies in that the 7190 has no idea what service the client wants unless a one-to-one mapping of service types to host names is made in the configuration. In this example scenario it would be easy to lump both the HTTP and HTTPS services together in the configuration for the hostname www.div1.mstd-ex.com. But a problem could occur if one of the services ever failed at a site; the others are still available. Even though one service has failed, the other is still available and all that is returned to the client is the IP address. The subsequent attempts by the client to use the referred address fails because it is asking for a service that is unavailable at that site. The solution requires a little more work in the host Web pages, but allows full advantage to be taken of the service awareness of the 7190. If unique hostnames are used for each service type, this problem never occurs. Note that if the load balancers are either Intel® NetStructure™ 7180s or are fronted by Intel® NetStructure™ 7110s, there is less of an issue with combining HTTP services with HTTPS services. Most of the traffic ever reaching a server would be HTTP.

In this scenario the services available on a single Web site have been divided into three different hostnames: www (HTTP), wwwsecure (HTTPS), and ftp (FTP). Another advantage of dividing the service types like this is that each hostname can be configured to use a different balancing method. Typically FTP traffic is fewer connections, but longer connection times. This is ideal for balancing by Least Connections. Secure traffic (HTTPS) or layer 7 load

balancing (Rich Mode) can place a heavy burden on the load balancers. This is ideal for balancing by CPU Utilization. Layer 4 load balancing is typically many short duration connections. In this case response time can be used as a direct measure of the actual server farms loading. This is ideal for balancing by Response Time.

The mapping of services to hostnames is also the easiest place to designate a service standby. If the service had been designated as *standby* in the agent record when it was first configured, it would have no effect. The **standby** command for an agent or ISV Group is a shortcut to placing that service in standby in all the hostnames that use that service at the time the command is issued.

```
config dns zones div1.mstd-ex.com hostnames
create www
www
method avgresp
siteservices
map site1:10.1.1.100:80
map site2:10.1.2.100:80
map backupsite:10.1.4.100:80
backupsite:10.1.4.100:80 standby
config dns zones div1.mstd-ex.com hostnames
create wwwsecure
wwwsecure
method cpu
siteservices
map site1:10.1.1.100:443
map site2:10.1.2.100:443
map backupsite:10.1.4.100:443
backupsite:10.1.4.100:443 standby
config dns zones div1.mstd-ex.com hostnames
create ftp
ftp
method conn
siteservices
```

```
map site1:10.1.1.102:21
map site2:10.1.2.102:21
map backupsite:10.1.4.102:21
backupsite:10.1.4.102:21 standby
```

Step 5. Add host for second zone and map its services.

```
config dns zones div2.mstd-ex.com hostnames
create www
www
method flash
siteservices
map site1:10.1.1.103:80
map site2:10.1.2.103:80
map site3:10.1.2.103:80
map backupsite:10.1.4.103:80
backupsite:10.1.4.103:80 standby
```

Step 6. Save and activate the configuration.

For a discussion of what is actually happening in this step see *Scenario 1, Part 1, Step 6.*

```
save first-cfg
commit all
```

Step 7. Configure the Secondary 7190s.

For this scenario the primary 7190 is the 7190 located at site1. All of the other 7190s are secondaries to this single primary. For details on how to configure a secondary see *Scenario 1, Part 1, Step 7*.

Step 8. Delegate authority to the 7190s.

See *Scenario 1, Part 1, Step 8* for an example of the type of entries required in a Bind domain database file to delegate authority. In reality the Bind files for this scenario would be quite complex because it would involve multiple divisions of a large company. Attempting to address the type of issues that might be involved goes well beyond the scope of this scenario.

5 Boot Monitor

The Intel 7190 Boot Monitor Command Line Interface (CLI) allows you to configure boot options and manage boot configuration files. Typically, the Boot Monitor is used only during initial configuration or major reconfigurations, should the latter become necessary. Day-to-day operations are managed with the CLI. See the Chapter 2, “Theory of Operations,” for an overview of 7190 operations. See Chapter 6, “CLI Reference,” for details on specific commands.

General categories of tasks performed through the Boot Monitor are:

- Configure and display boot options, including the configuration file
- Manage the boot configuration file system
- Configure and change IP parameters

System Requirements

You can use any terminal or personal computer with a terminal emulator as the CLI command station.

The terminal must have the following features:

- 9600 bits per second, 8 data bits, 1 stop bit no parity, no flow control.
- Serial terminal emulation program such as Terminal or HyperTerminal® for Windows® NT or HyperTerminal for Windows 95 or 98.
- Cable and connector to match male DTE connector (DB-9).

Accessing the Boot Monitor

__NOTE:__ After configuring the 7190 in the Boot Monitor, you must enable __autoboot__ for the device to boot into normal operating mode.

To access the Boot Monitor Command Line Interface, interrupt the boot sequence by pressing a key at the following prompt:

```
Press any key to stop autoboot
```

In a few seconds the following prompt appears, confirming that the Boot Monitor is running:

```
monitor>
```

Boot Monitor Command Reference

The Boot Monitor contains the following commands:

Command	Description
autoboot	Use this command to enable or disable the Autoboot function. When Autoboot is enabled, during startup the 7190 prompts you to press a key to enter the Boot Monitor command line interface. If you ignore the prompt, startup concludes with the 7190 in normal operating mode (displaying the `Intel 7190#` prompt). When Autoboot is disabled, the startup sequence is interrupted and displays the Boot Monitor interface (displaying the `monitor>` prompt). Autoboot is enabled by default. To enable Autoboot, press Enter to accept the default "`enable`." To disable, enter **`disable`**, then press Enter. Example: `monitor>`**`autoboot`** `Autoboot? [enable]--->`

Command	Description

boot
 	
NOTE: *User-entered names and IP addresses in the example are for illustrative purposes only. The appropriate values for your installation may vary.*
	This command boots the 7190 using a specified configuration.
	
	Example:
	`monitor>`**`boot`**
	`Current active configuration`
	`----------`
	`Product: 7190`
	`Version: 3.0`
	`Patch Level: 0.0`
	`Build: D18`
	`----------`
	`Current time: Fri Mar 31 14:04:56`
	`Current Config: default.cfg`
	`Hostname: intel7190`
	`Using DHCP: No`
	`IP Address: 10.1.1.11`
	`Netmask: 255.255.255.0`
	`Default Route: 10.1.1.1`
	`Domain: xyz-ex.com`
	`Primary nameserver: 10.1.1.101`
	`NTP: Enabled`
	`Servers: 10.1.1.2`
	`NIC setup: auto`
	`Autoboot: Enabled`
	`Boot timeout: 5 (seconds)`
	
	`Boot current configuration? [y]`
	`Please stand by, the system is being rebooted.`

delete	This command deletes the specified configuration file from 7190. Example: `monitor>`**`delete`** `Enter the configuration file to delete [] --->` **`filename.cfg`**

Command	Description

dir	This command displays the list of saved boot configuration files.
	
	Example:
	`monitor>dir`
	`File name`
	`----------`
	`*default.cfg`

dhcp	This command allows you to enable or disable the use of DHCP by the 7190. When DHCP is enabled, the 7190 receives its configuration parameters from the DHCP server at startup. When DHCP is disabled, the 7190 ignores the DHCP server, and so must be manually configured at startup. Respond to the prompt with **y** to enable, respond with **n** to disable. DHCP is disabled by default.
	
	Example:
	`monitor>dhcp`
	`Do you wish to use DHCP? [n]--->y`
	
	Press Enter to accept the default, **n** to disable DHCP, or enter **y**, then press Enter to enable.

dns	Use this command to specify the domain and (optionally) nameserver(s). The 7190 prompts you for the required information.
	
	Syntax:
	`monitor>dns`
	
	Example:
	`monitor>dns`
	`Enter domain ("-" to delete)`
	`[somedomain.com] --->somedomain.com`
	`Primary Name Server (<return> to end)`
	`[209.218.240.1] --->209.218.240.1`
	`Secondary Name Server (<return> to end "-" to delete)`
	`[] --->`

Command	Description
factory_reset ***NOTE:*** *`factory_reset` does not delete saved configuration files.* ***CAUTION:*** *This command rewrites the default configuration to the* ***default.cfg*** *configuration file.*	This command resets system to factory defaults. Values affected by this command are: • Entire current DNS configuration is deleted • Route parameters • CLI parameters • IP address • Default route • Hostname • Domain • Name servers • DHCP is disabled • Autoboot is set to “enabled”
halt	This command halts the 7190 system.

Boot Monitor Command Reference

Command	Description
help	This command lists all Boot Monitor commands or optionally displays syntax for a specified command. Example: `monitor>`**`help`** `autoboot` Enable or disable autoboot `boot` Boot saved configuration `delete` Delete a saved configuration file `dhcp` Use DHCP to configure system `dir` Directory of saved config files `dns` Configure domain and name server(s) `factory_reset` Reset system to factory defaults `halt` Use to halt 7190 system `help` Show list of available commands `host` Set host name `info` Show system status `ip` Set IP address `load` Load a specified configuration `netmask` Set netmask `nic` Configure network interface card `route` Set default route `save` Save the current configuration `setdate` Set the real-time clock `setup` Configure unit `show` Show saved configuration info `version` Display software version info

Boot Monitor Command Reference

Command	Description

info	This command displays the current boot configuration.
	
	Example:
	`monitor>`**`info`**
	`Current active configuration`
	`----------`
	`Product: 7190`
	`Version: 3.0`
	`Patch Level: 0.0`
	`Build: D18`
	`----------`
	`Current time: Thu Mar 31 12:04:39 2000`
	`Current Config: default.cfg`
	`Hostname: www`
	`Using DHCP: No`
	`IP Address: 10.1.1.11`
	`Netmask: 255.255.254.0`
	`Default Route: 10.1.1.1`
	`Domain: xyz-ex.com`
	`Primary nameserver: 10.1.1.10`
	`NIC setup: auto`
	`Autoboot: Enabled`
	`Boot timeout: 5 (seconds)`

ip	Use this command to specify the IP address of the 7190. Example: `monitor>`**`ip`** `Enter IP address [10.1.1.11] --->`**`10.1.1.111`**

load	Load a previously saved configuration file into memory.
	
	Example:
	`monitor>`**`load`**
	`Do you want to load a saved configuration? [n] --->`**`y`**
	`Configuration file name? [savedcnfg.cfg] --->`
	`Configuration loaded: savedcnfg.cfg`

Boot Monitor Command Reference

Command	Description
netmask	Use this command to specify the netmask. Example: `monitor>`**`netmask`** `Enter Netmask [255.255.254.0] --->`**`255.255.254.0`**

nic	Use this command to configure network interface card (NIC) parameters. Assurance of compatibility with some older switches, hubs, or routers, may require that you directly specify the Ethernet speed and duplex mode of the network interface card for the 7190. The **nic** command, available at the serial console, allows you to specify these characteristics.
	
	Example:
	`monitor>`**`nic`**
	`Auto config NIC card? [y] --->`**`n`**
	`1 - 100BaseTx`
	`2 - 10BaseTx`
	`Select Media Type (1 or 2): [1] --->`**`1`**
	`Use Full Duplex? [y] --->`**`y`**
	`Done Ether config: 100basetx,full_duplex`

route	Use this command to specify the default route (gateway). Example: `monitor>`**`route`** `Enter default route [10.1.1.1] --->`
save	Use this command to save the current configuration. Changes made during the current Boot Monitor session are lost unless you use the **`save`** command.

Command	Description

settime
 	
NOTE: *Flash does not work correctly if* ***settime*** *is not configured.*
	Use this command to configure the date and time of the 7190. One way to configure this is by using the Network Time Protocol (NTP). The user is prompted if NTP should be used, and is then prompted for IP addresses of the NTP servers. Be sure that the selected NTP servers are a reliable source for NTP time and that the NTP server latency is less than 20 milliseconds. If NTP is not used, then the date and time are configured manually.
	
	When you say no for "Use NTP?" the setdate prompts are displayed. When you specify yes, you are prompted for the NTP server address(es).
	
	Example:
	`monitor>`**`settime`**
	`Use NTP? [y] --->`**`n`**
	`Warning: Load Balancing Method FLASH will not work without NTP`
	`The current time is now: Wed Jan 12 20:23:53 2000`
	`Enter the year (YYYY): [2000] --->`
	`Enter the month (MM): [01] --->`
	`Enter the day (DD): [12] --->`
	`Enter the hour (HH): [20] --->`
	`Enter the minute (MM): [23] --->`
	`Enter the seconds (SS): [53] --->`
	`Wed Jan 12 20:23:53 2000`
	`Network Initialization...`
	`Application Initialization...`
	`monitor>`**`settime`**
	`Use NTP? [y] --->`**`y`**
	`Enter Name or IP address of NTP server: []`
	`Enter an additional IP address of an NTP server or <return> to end [] --->209.218.240.1`
	`Enter an additional IP address of an NTP server or <return> to end [] --->`
	`monitor>`
	
	When logging in to CLI, system date/time is displayed. If NTP is enabled and operational, NTP information is also be displayed.

Command	Description

setup	This command initiates the setup procedure of the 7190. The system displays prompts for all inputs necessary to initialize system.
	
	Example:
	`monitor>`**`setup`**
	`Auto config NIC card? [n] --->`**`y`**
	`Done Ether config: auto`
	`Enter hostname [nsb-9] --->`
	`Autoboot? [enable] --->`
	`Enable DHCP? [n] --->`
	`Enter domain ('-' to delete) [mysite_ex.com] --->`
	`Primary name server ('-' to delete) [10.1.1.10] -->`
	`Add additional name server (<return> to end) [] --->`
	`Enter IP address [10.1.1.1] --->`
	`Enter Netmask [255.255.254.0] --->`

show ***NOTE:*** *Use the* ***dir*** *command to display the list of saved configuration files.*	This command displays a specified saved boot configuration file. Type **show**, then the name of the configuration file you wish to view. Example: `monitor>`**`show`** `Configuration file name? [] --->`**`<filename>`**

Notes

6 CLI Reference

The Intel® NetStructure™ 7190 Multi-Site Traffic Director is fully configurable through the Command Line Interface (CLI). The CLI is accessible either through Telnet to the 7190, or the serial port. Commands exist in a logical hierarchy. This chapter contains a summary command list, illustrations of the command tree structure, and a comprehensive reference with descriptions of all commands, their parameters, and if applicable, examples of their output display.

Environment

Editing the Command Line

The 7190's CLI provides many key combinations for ease of editing. These are described in Table 6-. The list is also available in the CLI. Type **help ttychars** and press Enter.

CTRL-A	Move insertion point to beginning of line
CTRL-B	Move insertion point back one character
CTRL-C	Prompts to stop the currently running function
CTRL-D	Delete character under cursor
CTRL-E	Move insertion point to end of line
CTRL-F	Move insertion point forward one character
CTRL-H	Backspace
CTRL-L-<TAB>	Show all possible completions of the current command branch at the current level
CTRL-L	Clear screen
CTRL-N or Down Arrow	Next item in Command History (see "Command History" below)
CTRL-P or Up Arrow	Previous item in Command History
CTRL-R	Reverse Command History search
CTRL-S	Forward Command History search
CTRL-T	Transpose character over cursor with preceding character
CTRL-U	Delete from cursor to beginning of line
CTRL-W	Delete from cursor to beginning of word
<TAB>	Display all possible commands and levels available from current level, except global commands and dynamic nodes.
CTRL-_	Undo the last character
Esc-<	Display beginning of Command History
Esc->	Go to end of Command History
Esc-Backspace or Esc-CTRL-H	Delete previous word
Esc-B	Move insertion point back one word
Esc-C	Capitalize letter and move to end of word
Esc-D	Delete from cursor to end of word
Esc-F	Move insertion point forward one word
Esc-L	Make letter lower case and move insertion point to end of word
Esc-U	Capitalize entire word
Insert	Toggle insertion mode (insert or overwrite)

Key Combinations

Command History

The 7190's CLI records recently executed commands and allows you to review them.

history <n>

With no parameter <n> specified, **history** displays the last ten commands entered by the user. The integer <n> specifies the history index number. When <n> is specified on the command line, the ten commands executed before that of the specified index number are displayed.

! <n> or h <n>

NOTE: *You must include a space between the "!" or "h" and the history index number.*

Executes the command beginning at the specified history index number.

Pipes

Any command can be piped to either **grep** <**grepstring**> or **more**.

- Output display of commands piped to **grep** is limited to lines containing <grepstring>.
- Output of commands piped to `more` appears a page at a time for easier readability.
- Pipes can be cascaded (typically with a final pipe to `more`).
  Example: `config sys info | grep telnet | more`
- Multiple grep commands can be cascaded to search for multiple words.
  Example: `config sys info | grep telnet | grep port`

NOTE: *Do not enclose the search target in quotes.*

Online Help

7190 provides online help in the following forms:

- Type `help` to describe help features.
- Type **help ttychars** to display a list of special terminal editing characters.

- Type **help** <**command**> for a description of a specific command or, if relevant, a list of sub-commands you can enter from within <command>.
- Type**?** to display a path list of commands and parameters available from the current prompt or <command> forward.
- Typing**?** or **help** as one of a command's parameters, i.e., <command>, displays help regarding the parameters available for <command>.

Command Line Syntax

The CLI uses the following syntax:

Angled brackets (<>)	Angled brackets designate where you enter variable parameters.
Straight brackets ([ ])	Choices of parameters appear between straight brackets, separated by vertical bars.
Braces ({})	Optional commands or parameters appear between braces.
Bold	Commands shown as they are entered after the CLI prompt appear in **bold** type. (The prompt appears in normal typeface to distinguish it from the command text.)
Vertical bar (|)	Separates choices of input parameters within straight brackets. You may choose only one of a set of choices separated by the vertical bar. (Do not include the vertical bar in the command.)

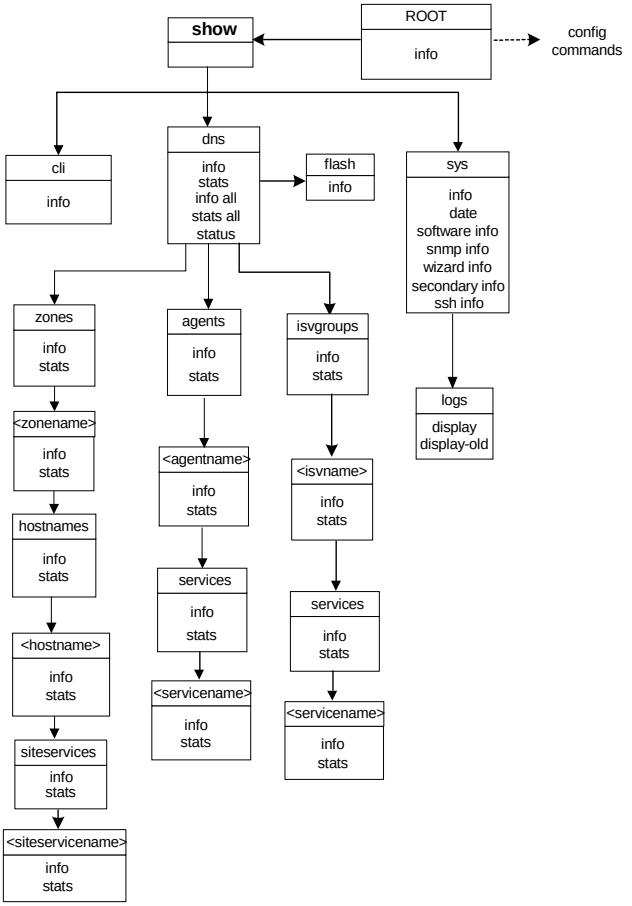
Command Line Syntax

CLI Command Summary

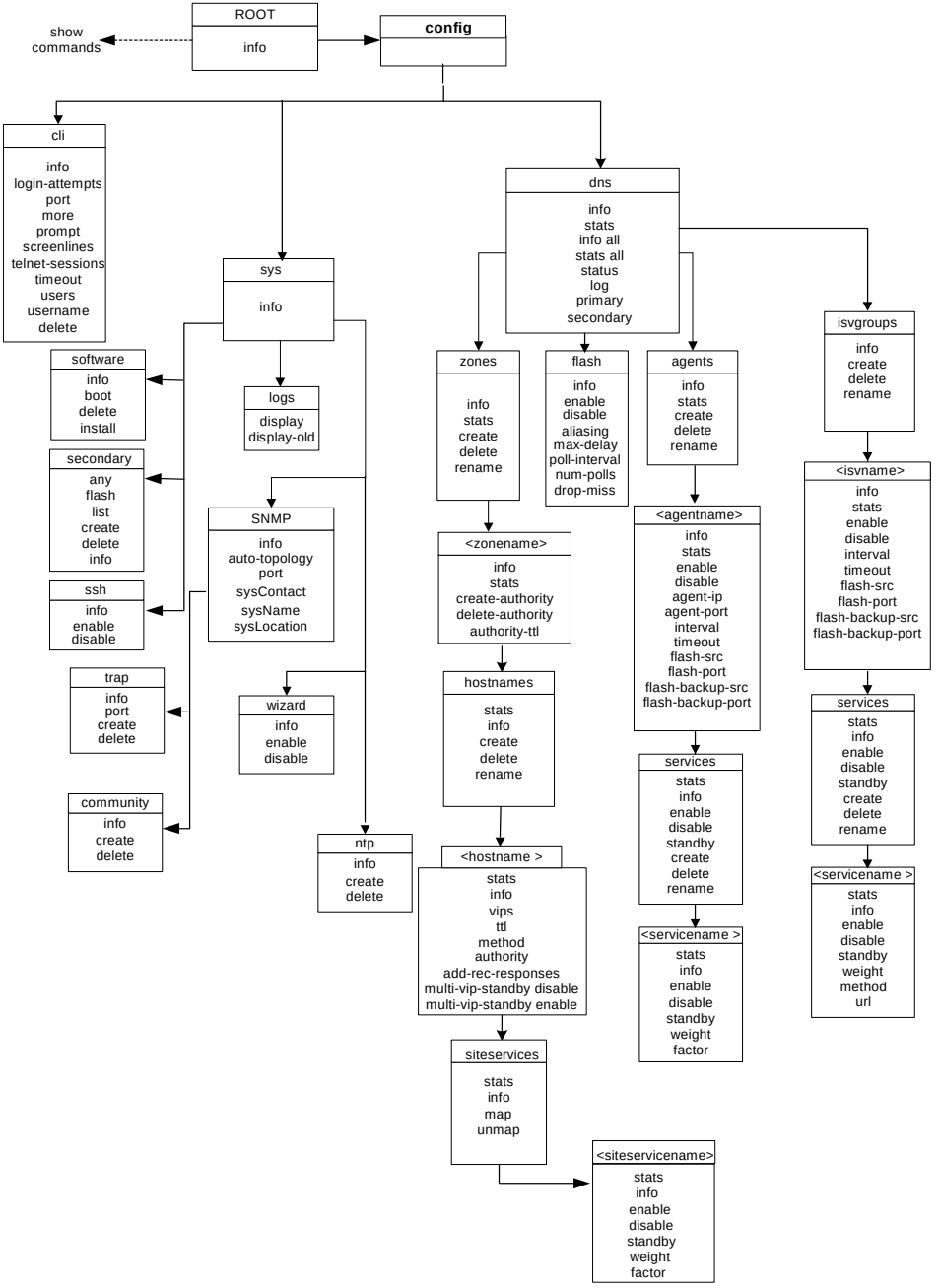
This section contains diagrams and lists of the 7190's CLI commands categorized by function. Complete details of CLI commands appear in the command reference section of this chapter.

Objects and Parameters

The following figures illustrate the **show** and **config** branches of the CLI-configurable objects and their relationships to one another within the 7190.



Command Tree (Show)



Command Tree (Config)

Global System Commands

```
?
!<n> or h<n>
!!
… | grep
… | more
arp
back (also box, top, toplevel)
box (also back, top, toplevel)
commit all
commit local
clearstats
dbpr
exit (also logout, quit)
halt
help
history
info
logout (also exit, quit)
netstat
nslookup
ping
quit (also exit, logout)
reboot
revert
factory-default
start-wizard
top (also back, box, toplevel)
toplevel (also back, top, box)
traceroute
who
```

File Management Commands

```
cat
copy
dir
get
put
remove
restore
restore-verbose
save
```

CLI Commands

NOTE: The **config info** *commands display uncommitted configuration information that is inactive. The* **show info** *commands display the active configuration information. A* **commit** *command is necessary before any* **config** *commands become active, after which the* **show info** *and* **config info** *commands displays matching information.*

```
config cli
    info
    login-attempts
    more
    port
    prompt
    screenlines
    telnet-sessions
    timeout
    username <username> password <password> level
    users
    delete
```

System Commands

```
config sys
    info
    logs display
    logs display-old
    ntp create <ntpserver>
    ntp delete <ntpserver>
    ntp info
    secondary info
    secondary any
    secondary flash
    secondary list
    secondary create <IP>
    secondary delete <IP>
    software info
    software boot
```

```
software delete
software install
secondary info
secondary any
secondary flash
secondary list
secondary create <IP>
secondary delete <IP>
ssh info
ssh enable
ssh disable
wizard info
wizard enable
wizard disable
```

SNMP Commands

config sys snmp

```
info
auto-topology <enable|disable>
port <#>
sysContact <contact person>
sysName <system name>
sysLocation <system location>
community info
community create <community string> ip <IP
address> rights <snmp rights>
community delete <string> ip [<IP
address>|any]
trap info
trap port <trap port>
trap create <IP address> community <community
string>
trap delete <IP address> community <community
string>
```

DNS Commands

config dns

```
stats
stats all
status
info
info all
```

```
   log
   primary
   secondary
config dns agents
   info
   stats
   metrics
   metrics <IP address> port <port#>
   create <agentname> ip <IP address>
   delete <agentname>
   rename <agentname> new <agentname>
config dns agents <agentname>
   info
   stats
   metrics
   metrics <IP address> port <port#>
   enable
   disable
   agent-ip
   agent-port
   interval
   timeout
   flash-src
   flash-port
   flash-backup-src
   flash-backup-port
config dns agents <agentname> services
   info
   stats
   enable
   disable
   standby
   create <servicename>
   delete <servicename>
   rename <servicename> new <servicename>
```

config dns agents <agentname> services <servicename>
- info
- stats
- enable
- disable
- standby
- weight
- factor

config dns isvgroups
- info
- create <isvname>
- delete <isvname>
- rename <isvname> new <isvname>

config dns isvgroups <isvname>
- info
- stats
- enable
- disable
- interval
- timeout
- flash-src
- flash-port
- flash-backup-src
- flash-backup-port

config dns isvgroups <isvname> services
- info
- stats
- enable
- disable
- standby
- create <servicename>
- delete <servicename>
- rename <servicename> new <servicename>

```
config dns isvgroups <isvname> services
<servicename>
   info
   stats
   enable
   disable
   standby
   weight
   method <probemethod>
   url <url>
config dns zones
   info
   stats
   create <zonename>
   delete <zonename>
   rename <zonename> new <zonename>
config dns zones <zonename>
   info
   stats
   create-authority <authorityname> ip
   <ipaddress>
   delete-authority <authorityname>
   authority-ttl
config dns zones <zonename> hostnames
   info
   stats
   create <atypehostname>
   delete <atypehostname>
   rename <atypehostname> new <atypehostname>
config dns zones <zonename> hostnames <hostname>
   info
   stats
   ttl
   method
   authority
   add-rec-responses <addrecrespval>
   multi-vip-standby enable
   multi-vip-standby disable
```

config dns zones <zonename> hostnames <hostname> siteservices
- info
- stats
- map
- unmap

config dns zones <zonename> hostnames <hostname> siteservices <siteservicename>
- info
- stats
- enable
- disable
- standby
- weight
- factor

config dns flash
- info
- enable
- disable
- aliasing
- max-delay
- poll-interval
- num-polls
- drop-miss

Show Commands

show cli info
show sys
  info
  date
  ntp info
  secondary info
  snmp info
  ssh info
  logs display
  logs display-old
  software info
  wizard info
show dns
  info
  flash info
  stats
  info all
  stats all
  status
show dns zones
  info
  stats
show dns zones <zonename>
  info
  stats
show dns zones <zonename> hostnames
  info
  stats
show dns zones <zonename> hostnames <hostname>
  info
  stats

show dns zones <zonename> hostnames <hostname> siteservices
  info
  stats
show dns zones <zonename> hostnames <hostname> siteservices <siteservicename>
  info
  stats
show dns agents
  info
  stats
  metrics
show dns agents <agentname>
  info
  stats
  metrics
show dns agents <agentname> services
  info
  stats
show dns agents <agentname> services <servicename>
  info
  stats
show dns isvgroups info
show dns isvgroups <isvname>
  info
  stats
show dns isvgroups <isvname> services
  info
  stats
show dns isvgroups <isvname> services <servicename>
  info
  stats

Global System Commands

Command	Description
?	Displays all the commands at the command level.
! (also **h, history**)	Displays the command history. Syntax: !<n> where: **n** is the command index number from history list.
!!	Repeats the last command.
arp	Displays 7190's ARP table.
back (also **..**)	Moves up one level in the CLI command tree.
box (also **top**)	Moves back to the beginning (root level) of the CLI branch command tree.
commit all	Saves changes and informs the DNS server of new configurations. It writes all changes to the disk and propagates the configurations to the secondary 7190s.
commit local	Saves configuration information on the local 7190 only (i.e., no information migrates to the secondary 7190s on the network.) This command is useful for testing new configurations.

Global System Commands

Command	Description

dbpr	Displays information on the active configuration down to the agent VIP level. This command is useful for assessing the effectiveness of the current balancing settings. Options consist of a hyphen and letter followed by a user-specified parameter or parameters. Syntax:
	`dbpr [host | agent | flash] {options}`
	where:
	`host` specifies that the command is to display information from a specified host.
	`agent` specifies that the command is to display information from a specified agent.
	`flash` specifies that the command is to display flash latency information between peers.
	
	Options:
	`-a agent_ip agent_port` limits the display output to information related to the load balancer identified by agent_ip and agent_port.
	`-h hostname` limits display output to information related to the host identified by hostname. Used together with the "-a" option, the "-h" option limits the display information to a specific service on the specified load balancer.
	`-z zonename` limits display output to information related to hosts within zonename. This option is ignored if combined with the "-h" option. Combining this option with the "-a" option constrains the display information to specific service(s) on the specified load balancer.
	`-f` overrides the default display limit of statistics and metrics only. Additional information displayed when "-f" is used includes weight, factor, TTL, and authority records.
	`-v vip_ip_address` limits output to information relating to VIPs with an IP address of ip_address. This option can be combined with the "-a", "-h", and "-z" options to display information related to a narrow subset of VIPs or even a single VIP. For example:
	`dbpr host -v 10.234.2.2 -h www.foo-ex.com -a 192.168.16.3 1999`

Command	Description
dbpr (cont'd)	Displays a single VIP- the one associated with host www.foo-ex.com whose IP address is 10.234.2.2 and is on the load balancer at 192.168.16.3:1999 **-c** causes the referral statistics associated with all displayed VIPs to be cleared following the display.
exit	Exits the CLI.
halt	Shuts down the 7190 preparatory to power off. If you wish to return the 7190 to operational mode from the halted state, you must manually reboot using the switch labeled "Reset" on the rear panel.
help	Displays help for the CLI.
history, (also !, h)	Displays the command history list or recalls a command by index number from the history list. Syntax: `history {<n>}` where: **n** is the command index number from the history list

Global System Commands

Command	Description
info	Information is displayed one page at a time if the file size is greater than 500K even when **more** (‘paging’) is disabled. This **info** command (at the root level) displays only current configurations, i.e., ‘committed’ changes (performed in the Config branch). This is the same information displayed from **info** commands on the Show branch of the CLI commands. **System Information** • Including the 7190’s unit identifier, MAC address, IP address, Netmask, Broadcast, Default Route, and Nameservers. **SNMP Information** • Including SNMP state (running or stopped), if auto-topology state (enabled or not), agent port, SysName, SysLocation, Community information, Trap information **Software Information** • For each installed version: Image index number, Product description, Version number, Patch number, Build number **CLI Information** • Number of concurrent Telnet sessions allowed, Root prompt, (number allowed of) Login attempts, More (‘paging’) state, (number of) Screenlines, System ID, CLI Timeout value, CLI port number, Wizard state (enabled or disabled) **NTP Servers Information** • Displays information about any configured NTP servers. **DNS Information** • Primary or secondary (state), Logging state, Flash Information (Flash state, Polling Interval, Max Broadcast Delay, aliasing state, Number of Polls, Drop Misses), Agent information and services configured under each agent, ISV Group information and services under the ISV, Zone information, Hostname and information (load balancing method), and Site Services information.
logout	Exits the current logged-in session.

Global System Commands

Command	Description
netstat	Displays the 7190's routing tables.
ping	Tests the network connection to another networking device. It sends an ICMP packet from the 7190 to the target device; when it receives the packet, it sends a ping reply. When the 7190 receives the reply, it displays a message indicating that the specified IP address is alive. If the unit receives no reply, it displays a message indicating that the target device is not responding. Syntax**:** `ping <ipaddress | hostname>` where: **`ipaddress`** is the IP address of the other networking device. **`hostname`** is the host name of the other networking device.
quit	Exits the current session.
reboot	Reboots the 7190.
revert	Returns the configuration to the last committed configuration.
factory-default ***NOTE:*** *Only those parameters set within the CLI are affected.*	Resets the 7190 to its original factory configuration. Original factory settings are listed below. Networking parameters controlled through the Boot Monitor are not affected by the **`factory-default`** command. CLI factory settings: • Entire DNS configuration is deleted. • 7190 is set to primary. • Telnet port is set to 23. • Prompt is reset to product name. • Maximum Telnet sessions is set to 0. • Idle timeout is set to 900 seconds. • Maximum login attempts is set to 3.
start-wizard	Starts the Quick Start Wizard, which is an automated, interactive system configuration tool.
toplevel (also **box**)	Changes the prompt level to the system top or box level.

Global System Commands

Command	Description
traceroute	Displays the route that packets travel to the network host.
who	Displays the list of all users currently logged in.

Global System Commands

File Management Commands

Command	Description
cat	Displays contents of the specified saved configuration file. Syntax: `cat <filename>` where: **`filename`** is the name of the file to be displayed.
copy	Copies an existing configuration file to a new file. Syntax: `copy <source> to <destination>` where: **`source`** is the name of the original file. **`destination`** is the name of the target file.
dir	Displays a list of saved configuration files. Also displays the last loaded configuration file.
get	Retrieves a configuration file from a TFTP server. Because the TFTP protocol has no user-login or validation, sites employing it typically enforce some file access restrictions. Such restrictions are specific to each site and vary widely in scope and methods. Syntax: `get <TFTP URL>` where: **`TFTP URL`** is the address of the tftp server from which you wish to retrieve the configuration file Example: get tftp://192.168.30.2/ tftpboot/get.cfg This helps to save configuration files outside the box.

File Management Commands

Command	Description
put	Transfers a configuration to the specified remote file or directory. If the remote-directory form is used, the remote host is assumed to be a UNIX device. Because the TFTP protocol has no user-login or validation, sites employing it typically enforce some file access restrictions. Such restrictions are specific to each site and vary widely in scope and methods. Syntax: `put <filename> to <TFTP URL>` where: **`TFTP URL`** is the address of the tftp server to which you wish to send the configuration file. **`filename`** is the name of the file to send. Example: put default.cfg to tftp://192.168.30.2/tftpboot/default.cfg
remove	Removes a configuration file. Syntax: `remove <filename>` where: **`filename`** is name of the configuration file to be removed.
restore	Restores a CLI configuration from a previously saved file. (See **save**.) Syntax: `restore <filename>` where: **`filename`** is the name of the configuration file to be restored. (The default file name is `default.cfg`.) Execute the command **`commit local`** or **`commit all`** to activate the restored configuration.
restore-verbose	As **`restore`** above, but displays each line of the restored file.

File Management Commands

Command	Description
save ***NOTE:*** *Username commands are not valid in configuration files, i.e.,* ***`save`*** *and* ***`restore`*** *operations do not include username data. Use the command* ***`config cli username`*** *to restore user names and passwords.*	Saves the current CLI configuration to a file of the specified name. This information is saved in a text file. (See also **restore**.) Syntax: `save <filename>` where: **`filename`** is the file name under which the configuration is stored. (The default file name is "default.cfg.")

File Management Commands

Configuration Commands

Config CLI Commands

Command	Description
config cli	Changes the prompt level to **`config cli`**.

Config CLI Commands

Command	Description

info	Displays the status of all variables at the `config cli` level. Information displayed:
	• Number of concurrent telnet sessions allowed
	• Root prompt
	• Number of login attempts allowed
	• More ('paging' enabled/disabled)
	• Number of screenlines
	• System ID
	• CLI timeout (number of timeouts)
	• CLI port (port number)
	Example:
	`Telnet sessions: 0`
	`Root prompt: Intel_7190`
	`Login attempts: 3`
	`More: disabled`
	`Screenlines: 25`
	`System Id: 7190`
	`CLI timeout: 900`
	`CLI Port: 23`

config cli delete	Deletes a user. Syntax: `config cli delete <username>` where: **`username`** is the username of the user you wish to delete.
login-attempts	Allows you to specify the maximum allowable number of failed login attempts before closing the connection on a Telnet session. Syntax: `config cli login-attempts <tries>` where: **`tries`** is a number from 1 to 30.

Config CLI Commands

Command	Description
more ***NOTE:*** *If information is greater than 500,000 bytes, the display is automated to display one page at a time.*	This paging command allows you to set scrolling of the output display to one page at a time or to continuous display. Syntax: `config cli more [enable | disable]` where: **`enable`** allows you to scroll one page at a time. **`disable`** results in continuous scrolling.
port	Specifies the Telnet port on which the CLI runs. Syntax: `config CLI port <port>` where: **`port`** is a valid port. Valid ports are port 23 or any port between 1024 and 65535. The default is port 23.
prompt	Changes the root level prompt. Syntax: `config cli prompt <prompt>` where: **`prompt`** is the new prompt name. The default prompt is an abbreviation of the product's name, e.g., "Intel_7190." The default prompt can be restored by entering "" as the prompt name.
config cli screenlines	Specifies the number of lines in the output display. Syntax: `config CLI screenlines <nlines>` where: **`nlines`** is the number of output lines (8 to 64). The default number of screenlines is 25. If 'nlines' does not match the lines in the screen, output is not displayed properly.

Config CLI Commands

Command	Description
telnet-sessions ***NOTE:*** *If you set the number of sessions to 0, you are disabling all future Telnet sessions to the 7190. To reset Telnet, you must access the device through the serial port and login, then change the Telnet session count from 0, to a number from 1 to 8*	Sets the allowable number of concurrent inbound remote CLI login sessions. Syntax: `config CLI telnet-sessions <nsessions>` where: **`nsessions`** is the number of allowed sessions (0 to 8). The default number of sessions is 0. .
timeout ***NOTE:*** *Too small of a timeout value renders the CLI useless.*	Sets or changes the idle timeout period before automatic logout for CLI sessions. The timeout value can be set to 0, which specifies no timeout. To set a value, use the range 30 to 65535 seconds. Syntax: `config CLI timeout <seconds>` where: **`seconds`** is the timeout period in seconds (0, or a range of 30 to 65535). The default is 900 seconds (15 minutes).

Config CLI Commands

Command	Description

config cli username
 	
NOTE: *Username commands are not valid in configuration files, i.e.,* ***save config*** *and* ***restore config*** *operations do not include username data.*
	Add, change, or delete the login or password. The default user name, "admin" cannot be deleted.
	Syntax:
	To delete a user:
	`config cli username [delete] <name>`
	To add or update a user:
	`config cli username <name> password <password> level <ro | rw | rwa>`
	where:
	`name` is the login name. (Must be from four to sixteen characters with no spaces.)
	`password` is the password. (Must be from four to sixteen characters with no spaces.)
	`level` is the authorization level for the user:
	• **`ro`** = read only (user can read, but cannot modify data)
	• **`rw`** = read & write (user can read and modify data, but cannot add or delete users)
	• **`rwa`** = read & write admin (user can read and modify data, and can add and delete users)

users	View all usernames and their access levels that exist in the system. Syntax: `config cli users`

Config CLI Commands

Config Sys Commands

Command	Description
config sys	Changes the prompt level to the System Config branch.

info
NOTE: *The default route is the same as the default gateway.*
	Displays the 7190's current system information.
	For example:
	`System Id:`
	`MAC Address: 0:90:27:73:f0:e4`
	`IP Address: 10.1.10.227`
	`Netmask: 255.255.0.0`
	`Broadcast: 10.1.255.255`
	`Default Route: 10.1.1.1`
	`Nameservers: mysite-ex.com`
	`10.1.1.10`

logs display	Displays the contents of the specified log file.
	Syntax:
	`config sys logs display`
	`<all|dns|ntp|system|monitor|stats>`
	where:
	all - displays all log messages
	dns - displays DNS activity and health monitor information on this 7190.
	ntp - displays ntp messages
	system - displays system messages
	monitor - displays monitoring messages
	stats - displays statistical information

logs display-old	Displays the contents of the old log file.
	Syntax:
	`config sys logs display-old`
	`<system|dns|ntp|stats|all>`

software	Changes the prompt level to **`config sys software`**.

Config Sys Commands

Command	Description

config sys
software info
	Displays all images that have been installed in the 7190. This includes the index number, the product name, the version number, the patch number, the build number and the word "Running" next to the image that is currently active on the 7190.
	For example:
	`Index Product Version Patch Build`
	`----- ------- ------- ----- -----`
	`1 Intel_7190 3.1 0.0 D3 Running`
	`2 Intel_7190 3.0 0.1 D6`

software install ***NOTE:*** *Save your configurations before installing or booting a new image. Up to five (5) images can be installed on a 7190.*	Download and install 7190 software through the FTP protocol. Once installed, images are selected for execution by using the command, **`config sys software boot.`** Syntax (ftp): `config sys software install <ftp url> {user <user name>} {password <password>}` where: **`url`** is a valid URL identifying the software image to download. It must be of the form ftp://<host>/<path_name>. **`user name`** is the user name to use for logging in during file transfer (ftp only). **`password`** is the password to use for logging in during file transfer (ftp only).
software boot ***NOTE:*** *Save your configurations before installing or booting a new image.*	Select a software image and reboot the system under that image. Syntax: `config sys software boot <index>` where: **`index`** is a valid index number of an installed software image, as displayed using the command, **`show sys software info`**.

Config Sys Commands

Command	Description

config sys
software delete
 	
NOTE: secondary *commands do not need to be committed to become active (they are in effect for any future connection attempts).*
	Delete old versions of the software from local storage. It can be used to free local storage to install a version update or product upgrade.
	Syntax:
	`config sys software delete <index>`
	where:
	`index` is a valid index number of an installed software image, as displayed using the command,
	`config sys software info`
	(also: `show sys software info`)

secondary ***NOTE: secondary*** *commands do not need to be committed to become active (they are in effect for any future connection attempts).*	Changes the prompt level to the **`config sys secondary`** branch.
secondary any	Allows any secondary 7190 to connect to the primary 7190. This command is executed on the primary 7190.
secondary info	Displays information about which secondary 7190s can connect.
secondary flash	Allows only secondary 7190s with an IP address in the Flash peer list to connect. This command is executed on the primary 7190.
secondary list	Displays only secondary 7190s configured using the **`config sys secondary create <ip>`** command.
secondary create <ip>	Adds addresses to the *config sys secondary* list. These are addresses of 7190s that can be connected as secondaries.
secondary delete <ip> ***NOTE:*** *Deleting an address prevents future connections for the specified address.*	Deletes addresses from the *config sys secondary* list.

Config Sys Commands

Command	Description
config sys **ssh info**	Displays the current status of SSH enable or disable. If the status was just changed, it reflects the changed status that is pending for the reboot.
ssh enable	Enables SSH connections the next time the box is rebooted.
ssh disable	Disables SSH connections the next time the box is rebooted.
config sys **wizard info**	Displays information about whether the Wizard is enabled or disabled. By default, Wizard is enabled.
wizard enable	Enables the Quick Start Wizard. The Quick Start Wizard is an automated, interactive method to configure the 7190. It is available only through the serial port if enabled after Boot Monitor.
wizard disable	Disables the Quick Start Wizard.
ntp create **<ntpserver>** ***NOTE:*** *If you used selected Flash load balancing in the Quick Start Wizard, you need to configure NTP.*	Adds an NTP server. Syntax: `ntp create <ntpserver>` where: **`ntpserver`** is the fully qualified hostname or the IP address of the Network Time Protocol Server.
ntp delete **<ntpserver>**	Deletes an NTP server. Syntax: `ntp delete <ntpserver>` where: **`ntpserver`** is the fully qualified hostname or the IP address of the Network Time Protocol Server.
config sys **ntp info**	Displays information about any configured NTP servers.

Config Sys Commands

Config Sys SNMP Commands

Command	Description
config sys snmp	Changes the prompt level to **`config sys snmp`**.
info	Displays information about SNMP agent port, sysContact, sysName, sysLocation and auto-topology
port	Allows you to specify the port on which the 7190 receives SNMP requests. Syntax: `config sys snmp port <agentport>` where **`agentport`** is a number between 5020 and 65535 (the default is 161)
auto-topology	Enables or disables operation of the auto-topology protocol. The default is `disable`. Syntax: `config sys snmp auto-topology [enable|disable]`
sysContact	Allows you to specify a value for the MIB-II variable sysContact. The default is null. Syntax: `config sys snmp sysContact <string>` where **`string`** is a string of displayable characters.
sysLocation	Allows you to specify a value for the MIB-II variable sysLocation. The default is null. Syntax: `config sys snmp sysLocation <system location>` where **`system location`** is a string of displayable characters.
sysName	Allows you to specify a value for the MIB-II variable `sysName`. The default is the hostname of the 7190. Syntax: `config sys snmp sysName <system name>` where **`system location`** is a string of displayable characters.
config sys snmp community info	Displays the community strings the 7190 is configured to accept, such as Community (name), IP address, and Rights. Rights are **`ro`** (read-only) and **`rw`** (read-write).

Config Sys SNMP Commands

Command	Description
community create	Specifies community strings that the 7190 accepts on incoming SNMP requests. Up to 10 community strings can be created. Syntax: `config sys snmp community create <string> ip [<IP address>|any] rights [ro|rw]` where **`string`** is the name of the community you wish to create, **`ip address`** is the IP address of the host from which you accept this community string. If `any` is specified, the community string is accepted on requests from any IP address. **`ro`** means the community string has read-only privilege. **`rw`** means the community string has read-write privilege. The default community strings are **`public any ro`** and **`private any rw`**.
community delete	Deletes a community string that the 7190 can accept on incoming SNMP requests. Syntax: `config sys snmp community delete <string> ip [<ip address> | any]` where: **`string`** is the name of the community string you wish to delete, and **`ip address`** is the IP address of the host from which you do not accept this community string. If `any` is specified, the community string does not accept requests from any IP address.
trap create	Allows you to specify the host to which 7190 sends SNMP traps. Up to 10 trap receivers can be created. By default the trap receiver list is empty, that is, no traps are sent. Syntax: `config sys snmp trap create <ip address> community <community string>` where **`ip address`** is the IP address of the host to which you wish to send SNMP traps. **`community string`** is sent with all traps sent to the IP address.
config sys snmp trap port	Specifies the trap port number. The port number is between 5020 and 65535. Default is 162. Syntax: `config sys snmp trap port <trap port>` where **`trap port`** is the designated number.

Config Sys SNMP Commands

Command	Description
trap delete	Deletes a host from the trap receiver list. Syntax: `config sys snmp trap delete <ip address> community <community string>` where **`ip address`** is the IP address of the host you wish to delete from the trap receiver list, and **`community string`** is an identifier associated with specified access rights.
trap info	Displays the trap receiver list of: • Trap ID Address • Trap Community

Config Sys SNMP Commands

Config DNS Commands

Command	Description
config dns	Moves you to the **`config dns`** command level.

config dns info	Displays DNS information.
	For example.
	`DNS Information`
	`Running as a Primary`
	`Logging is Disabled`

Config DNS Commands

Command	Description
info all	Displays all DNS information. For example: DNS Information Running as a Primary Logging is Disabled Flash Information: Flash State: Disabled Aliasing: Disabled Polling Interval: 10 Number of Polls: 100 Max Broadcast Delay: 500 Drop Misses: 3 Agent: 10.1.2.8 State: Enabled Metrics Interval:30 Metrics Timeout:15 Agent IP: 10.1.2.8 Agent Port: 1999 Primary Flash Src: Not Defined Primary Flash Port: 0 Backup Flash Src: Not Defined Backup Flash Port: 0 Zone: zone1.com Authority Records TTL: 86400 Host: host1.com Method: wrr TTL:60 Return Authoritative:Yes

Config DNS Commands

Command	Description

config dns stats	Displays the status of this 7190 and any connected secondary 7190s.
	For example:
	`Queries: 0 Queries/Sec: 0 Avg Queries/Sec: 0`
	`Referrals: 0 Refused: 0`
	`Unknown Zones:0 Unknown Hosts: 0`
	`Malformed: 0 Unsupported: 0`
	
	Queries - Total number of DNS queries received.
	Referrals - Total number of times that a particular service or group of services have been returned as the answer to a query.
	Unknown Zones - Total number of queries received for hosts in zones that the 7190 is authoritative for, but do not exist in the configuration.
	Malformed - Total number of received queries that violated the syntax rules for a proper DNS request packet.
	Queries/Sec - Total number of queries per second.
	Refused - Total number of received queries for information that is refused for policy reasons.
	Unknown Hosts - Total number of queries received for hosts in zones that the 7190 is authoritative for, but do not exist in the configuration.
	Unsupported - Total number of queries for unsupported DNS response types. For example requests for MX (mail) records would return Unsupported.
	Avg Queries/Sec - Average number of queries per second.

config dns stats all	Displays all statistics for this 7190. (See **`stats`** command for definitions.)
	For example:
	`Queries: 0 Queries/Sec: 0 Avg Queries/Sec: 0`
	`Referrals: 0 Refused: 0`
	`Unknown Zones:0 Unknown Hosts: 0`
	`Malformed: 0 Unsupported: 0`
	
	`Agent: 10.1.2.8 (Version 45.0.0.0)`
	`State: Connected CPU Util: 0% Connections/Sec:0`
	
	`Zone: zone1.com`
	`Queries: 0 Referrals: 0`
	
	`Host: host1.com`
	`Queries: 0 Referrals: 0`

Config DNS Commands

Command	Description
log ***NOTE:*** *Enabling logging may reduce the speed of DNS resolutions.*	Enables or disables logging. When logging is enabled, the DNS server logs details of the incoming queries, the balancing process for VIP selection, and the query response to the log file. Default: disabled. Syntax: `config dns log [enable|disable]`
status	If the 7190 is a primary, Displays the secondary 7190(s) to which it is currently connected. If the 7190 is a secondary, Displays the connection status to its primary.
primary ***NOTE:*** *Each primary can have simultaneous connections to as many as four secondary 7190s.*	Designate the device as the primary 7190. Connection to any unit previously designated as primary is lost when this command is executed. Default: enabled. Syntax: `config dns primary [enable|disable]` where: **`enable`** designates the 7190 as the primary.
config dns secondary ***NOTE:*** *Upon successful connection to the primary, all commands under* **config dns zones** *become unavailable to the secondary. Primary and secondary configurations are the same and are transferred to the secondary after every "commit" within the primary.*	Designates this unit as a secondary 7190. Syntax: `config dns secondary <primary ip address>` where: **`primary ip address`** is the address of the primary 7190 to which the current unit is subordinated as a secondary.

Config DNS Commands

Config DNS Agents Commands

Command	Description

info	Displays the configuration information of all agents in the 7190. Each 7190 may have up to 16 agents configured.
	For example:
	
	`Agent: 10.1.2.8`
	`  State: Enabled  Metrics Interval: 30`
	`  Metrics Timeout: 15`
	
	`  Agent IP: 10.1.2.8  Agent Port: 1999`
	`  Primary Flash Src: Not Defined`
	`  Primary Flash Port: 0`
	`  Backup Flash Src: Not Defined`
	`  Backup Flash Port: 0`

stats	Displays the statistical information of each agent configured under this 7190.
	For example:
	
	`Agent: load1 (Version 45.0.0.0)`
	`  State: Connected CPU Util: 5% Connections/Sec: 0`
	
	`Agent: load2 (Version Unknown)`
	`  State: Connected CPU Util: 0% Connections/Sec: 0`
	
	Information displayed:
	• Agent IP: (IP address of load balancer and version number)
	• Current State: (e.g., Connected or Disconnected)
	• CPU Utilization: (Percentage of CPU usage)
	• Connections Per Second

Config DNS Agents Commands

Command	Description

config dns agents metrics	Displays metrics information of all configured agents. If an IP address and a port number are specified, metrics for that agent is obtained.
	`config dns agents metrics <ip address> port <port>`
	where an optional agent IP address port can be specified, otherwise all metrics are returned. The standard agent port is 1999.
	Displays the following information for each listed agent:
	• Agent (name or address)
	• Version (version number of the agent software)
	• State (current status of the agent)
	• CPU Util (processor use)
	• Connections/Sec (number of connections per second established with this load balancer)
	For example:
	`Agent: load1 (Version 45.0.0.0)`
	`State: Connected CPU Util: 5% Connections/Sec: 0`
	`Agent: load2 (Version Unknown)`
	`State: Connected CPU Util: 0% Connections/Sec: 0`

create	Creates an agent with an IP address. Syntax: `config dns agents create <agentname> ip <ip address>` where: **`ip address`** is the address of the newly created agent. **`agentname`** is the name of the load balancer.
delete <agentname>	Deletes an agent from the agent list. Syntax: `config dns agents delete <agentname>` where: **`agentname`** is the name of the agent to be deleted. Only configured agents can be deleted.

Config DNS Agents Commands

Command	Description
config dns agents rename <agentname> new <agentname>	Changes the agent's current name to the name specified in the command line. Syntax: `config dns agents rename <agentname> new <agentname>` where: **agentname** (1) is the current name of the agent whose name you wish to change. **agentname** (2) is the new name to be assigned to the agent.

config dns agents <agentname> info	Displays configured information of the specified agent.
	For example:
	`Agent: 10.1.1.1`
	`State:Enabled Metrics Interval:30 Metrics Timeout:15`
	`Agent IP: 10.1.1.1 Agent Port: 1999`
	`Primary Flash Src: Not Defined Primary Flash Port:0`
	`Backup Flash Src: Not Defined Backup Flash Port:0`
	`Services:`
	`10.1.1.3:80`

stats	Displays the statistical information of the specified agent, including any services. Information displayed includes.
	• Agent Name and Version
	• State: (Connected state of agent)
	• CPU Util: (Processor Use)
	• Connection/Sec:
	• Service name(s): (IP address and port number)
	• Service referrals, response time, flash referrals, and connections/sec
	For example:
	`Agent: 10.1.1.1 (Version Unknown)`
	`State: Connected CPU Util: 0% Connections/Sec: 0`
	`Service: 10.5.5.5:90 (0 Servers)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`

Config DNS Agents Commands

Command	Description

config dns agents <agentname> metrics	Displays metric information for the specified agent.
	Syntax:
	`config dns agents <agentname> metrics`
	where:
	agentname is the name of the agent whose metrics you want to display.
	Information displayed:
	• Agent name
	• Agent Version Number (software version)
	• Agent State
	• CPU Utilization
	• Average Connections per Second (average established with this agent)
	• Any services and their respective statistics (IP address, port, referrals, etc.).
	Example:
	`Agent: 10.1.1.1 (Version Unknown)`
	`State: Connected CPU Util: 0% Connections/Sec: 0`
	
	`Service: 10.5.5.5:90 (0 Servers)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`

agent-port <port #> ***NOTE:*** *If the default value is changed, ensure that the agent is listening on the port number that is configured in order to establish a successful connection.*	Sets or change the TCP port number which is used to establish connection to the agent. `config dns agents <agentname> agent-port <port#>` where: **port#** is the TCP port number. Default is 1999

Config DNS Agents Commands

Command	Description
config dns agents <agentname> flash-src <ipaddress> ***NOTE:*** *At least one of the (up to 5) unique flash-source addresses must be the IP address of the 7190 itself.*	Configures the IP address of the peer flash sources. These include the IP addresses of this 7190 itself and additional 7190s if they exist. Up to five unique flash-source addresses can be configured among the sixteen possible agents.
flash-port <port#>	Sets or changes the UDP port number through which flash peers communicate to each other. The default port number is 2000.
flash-backup-src <ipaddress>	Configures a backup source address to which queries are routed, in the event of this 7190 not being functional. The backup source address is the IP address of another 7190 or a load balancer with a flash-agent configured.
flash-backup-port <port#>	Configures the port number with which the backup flash source communicates with its known peers. The default port number is 2000.
interval	Configures the interval at which metrics are gathered from the specified agent. The default is 30 seconds. Syntax: `config dns agents <agentname> interval <seconds>` where: **`agentname`** is the name of the agent whose metric-gathering interval you wish to set. **`seconds`** is an integer between 1 and 300 seconds.
config dns agents <agentname> timeout	Establishes the time that elapses during which the NCA waits for metrics from the specified agent before assuming the agent to be dead. The default value is 15 seconds. Syntax: `config dns agents <agentname> timeout <seconds>` where: **`agentname`** is the name of the agent whose metrics gathering timeout interval you wish to set. **`seconds`** is an integer between 1 and 300 seconds.

Config DNS Agents Commands

Command	Description
agent-ip <agentip>	Configures the IP address of the corresponding agent name.
enable	Enables communication with the agent. Default: enabled.
disable	Disables the agent. Services configured under these agents are no longer available for resolution.

config dns agents <agentname> services info	Displays information about any existing services. For example, when there are two services created:
	`Service: 10.1.2.8:90`
	`Service IP: 10.1.2.8 Service Port: 90`
	
	`Service: 10.2.2.3:80`
	`Service IP: 10.2.2.3 Service Port: 80`

stats	Displays statistics for all services for the specified agent. For example:
	`Service: 10.1.2.8:90 (0 Servers)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`
	
	`Service: 10.2.2.3:80 (0 Servers)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`

config dns agents <agentname> services create	Creates a service. Syntax: `create <svcname>` where: **svcname** is a VIP and port number (e.g., 10.1.2.8:80)
delete	Deletes a service. Syntax: `delete <svcname>` where: **svcname** is a VIP and port number (e.g., 10.1.2.8:80)

rename	Renames an existing service.
	Syntax:
	`rename <svcname> new <new svcname>`
	For example, to change the port number as part of a service name:
	`rename 10.1.2.8:80 new 10.1.2.8:90`

Config DNS Agents Commands

Command	Description
enable	Enables all services for all hosts which currently map to them.
disable	Disables all services for all hosts which currently map to them.
standby	Places on standby all services for all hosts which currently map to them.

config dns agents <agentname> services <svcname> info	Displays information about the specified service.
	For example:
	`services 10.2.2.3:80 info`
	Displays the following:
	`Service: 10.2.2.3:80`
	`Service IP: 10.2.2.3 Service Port: 80`

stats	Displays the statistics of the specified service.
	`Service: 10.2.2.3:80 (0 Servers)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`

config dns agents <agentname> services <svcname> enable	Enables the specified service for all hosts which currently map to it.
disable	Disables the specified service for all hosts which currently map to it.
weight	Sets a weight of an agent service. Services with higher weight are favored over services with lower weight. Syntax: `weight <weightnumber>` where **`weightnumber`** is between 1 and 255. Default is 1.
factor	Sets the threshold for an agent service based on the load balancing method (CPU/AVGRESP/LEAST CONN). Syntax: `factor <factornumber>` Where: **`factornumber`** is between 1 and 255. Default is 10

Config DNS Agents Commands

Command	Description
standby	Sets the mode of a service to standby for all hosts that currently map to it.

Config DNS Agents Commands

Config DNS ISV Groups Command

Command	Description
config dns isvgroups	Moves to the **`config dns isvgroups`** command level.

config dns isvgroups info	Displays configured information of all ISV Groups in this 7190. For example:
	`ISV Group: isv2`
	`State: Enabled Probe Interval:30 Probe Timeout:15`
	`Primary Flash Src:10.1.1.1 Primary Flash Port:2000`
	`Backup Flash Src: 10.1.1.2 Backup Flash Port: 2000`
	`ISV Group: isv3`
	`State:Enabled Probe Interval:30 Probe Timeout:15`
	`Primary Flash Src: Not Defined Primary Flash Port:0`
	`Backup Flash Src: Not Defined Backup Flash Port:0`
	Probe Interval: How frequently the services in an ISV group are polled for availability.
	Probe Timeout: How long to wait for a response to an ISV service availability poll.

create <isvname>	Creates an ISV group name. ISV name is the hostname of any generic load balancer that you wish to configure. For example: `create isv2` Creates the 'isv2' group.
delete <isvname>	Deletes a configured ISV group, specified by the ISV name.
rename <isvname> new <isvname>	Changes the name of an existing ISV group to the new one specified. For example: `rename isv2 new generic2` changes the name 'isv2' to 'generic2.'

Config DNS ISV-Groups Commands

Command	Description
config dns isvgroups <isvname>	Move to the command level of a specific ISV group.

info	Displays information of the ISV group specified by the ISV name.
	For example:
	`isvgroups isv2 info`
	Displays:
	`ISV Group: isv2`
	`State: Enabled Probe Interval:30 Probe Timeout:15`
	`Primary Flash Src: Not Defined Primary Flash Port:0`
	`Backup Flash Src: Not Defined Backup Flash Port: 0`
	`Services:`

stats	Displays statistical information on the specified ISV group.
enable	Enables the ISV group for all services under it. All ISV groups are enabled by default.
disable	Disables the specified ISV group. Services under this ISV group are not available after disabling.
flash-src <ipaddress> ***NOTE:*** *At least one of the unique flash-source addresses must be the IP address of this 7190.*	Configures the IP address of the peer Flash sources. These includes the IP addresses of this 7190 and additional 7190s if they exist. Five unique flash source addresses can be configured under each agent. For example: `flash-src 10.1.1.1`
flash-port <port#>	Sets or changes the UDP port number through which Flash peers communicate to each other. The default port number is 2000.
config dns isvgroups <isvname> flash-backup-src <ipaddress>	Configures a backup source address to which queries are routed, in the event of this 7190 not being functional. The backup source address is the IP address of another 7190 or a load balancer with a flash-agent configured. For example: `flash-backup-src 10.1.1.2`

Config DNS ISV-Groups Commands

Command	Description
flash-backup-port <port#>	Configures the port number with which the backup flash source communicates with its known peers. The default port number is 2000.
config dns isvgroups <isvname> services	Moves to the ISV services command level.

info	Displays configured information of all services for the specified ISV group.
	For example, with one service:
	`Service: 10.10.9.8:80`
	`Service IP: 10.10.9.8 Service Port: 80`
	`Probe Method: none`

stats	Displays statistical information for the specified service.
enable	Enables all services that are configured for this ISV group to all hosts that map to them. Default is enabled.
disable	Disables all services that are configured in this specified ISV group.
standby	Places all services in standby mode for the specified ISV group. Standby services are enabled when enabled services are unavailable.
create <servicename>	Creates a service where <servicename> is a VIP:port combination.
config dns isvgroups <isvname> services delete <servicename>	Deletes a service where **servicename** is a VIP:port combination.
rename <servicename> new <servicename>	Changes the servicename of an existing service to the newly specified.
config dns isvgroups <isvname> services <servicename>	Moves to a specific service command level.

Config DNS ISV-Groups Commands

Command	Description

info	Displays information, and limits information to one specified service.
	For example, a display could be:
	`Service: 10.10.9.8:80`
	`Service IP: 10.10.9.8 Service Port: 80`
	`Probe Method: none`

stats	Displays statistical information for the specified service.
enable	Enables the specific service for the hosts that map to it. All services are enabled by default.
disable	Disables the specific service for the hosts that map to it. All services are enabled by default.
standby	Configures this service to be standby for all hosts that map to it. Standby services are enabled when enabled services are unavailable.
weight <number>	Sets or changes the weight for this ISV service on this ISV group. Each service is assigned a weight based on the load balancing method and the load on the servers.
config dns isvgroups <isvname> services <servicename> method <probemethod>	Sets or changes the method to probe a service. The options are: • Ping • TCP • HTTP
url <url>	Specifies the file to retrieve when the probe method is HTTP. Pathname specifies the entire pathname from which the file is to be retrieved, relative to the root of the Webserver.

Config DNS ISV-Groups Commands

Config DNS Zones Commands

Command	Description
config dns zones	Moves to the DNS Zones level.

Config DNS Zones Commands

Command	Description

config dns zones info	Displays the names of all configured zones under this 7190. To display the names of committed zones only, use the command **`show dns zones info`**.
	Example:
	`Zone: zone1.com`
	`Authority Records TTL: 86400`
	
	`Zone: zone2.com`
	`Authority Records TTL: 86400`

config dns zones stats	Displays the number of queries and referrals performed by the DNS server for each committed zone under this 7190.
	Information displayed:
	• Zonename
	• Queries (number of queries for all committed hosts under this zone.)
	• Referrals (number of times that a host has been returned as an answer to a query)
	Example:
	`Zone: zone1.com`
	`Queries: 0 Referrals: 0`

create	Creates a zone. Zone names may not exceed 253 characters, (allowing at least one character for a hostname and one for the "." between the host name and the zone name. Up to 300 zones can be created. Zone names must be unique.
	Valid zone name characters are:
	• Alphanumerics (case insensitive)
	• Dot (.)
	• Hyphen (-)
	
	Syntax:
	`config dns zones create <zonename>`
	where:
	`zonename` is the name of zone to be created.
	Example:
	`mysite-ex.com`

Config DNS Zones Commands

Command	Description
delete ***NOTE:*** *This command also deletes all hosts and VIPs configured under the zone to be deleted.*	Deletes the specified zone from the zone list. Syntax: `config dns zones delete <zonename>` where: **zonename** is the name of the zone you wish to delete.
config dns zones rename	Changes the name of an existing zone. Hosts configured under that zone are unaffected. Syntax: `config dns zones rename <zonename> new <zonename>` where: **zonename** (1) is the current name of the zone you wish to rename. **zonename** (2) is the new name you wish to give to the specified zone.
config dns zones <zonename> info	Displays configuration information for the current zone. Syntax: `config dns zones <zonename> info` where: **zonename** is the name of the zone whose configuration information you wish to view. Information displayed: • Zone name • Authority TTL • Authority records (Authority Name and IP address) • Names of all hosts configured under this zone.

Config DNS Zones Commands

Command	Description

config dns zones stats	Displays the statistical information of the specified zone.
	Syntax:
	`config dns zones <zonename> stats`
	where:
	zonename is the name of the zone whose statistical information you wish to view.
	Example:
	`Zone: mysite-ex.com`
	`Queries: 0 Referrals: 0`
	`Host: host1.com`
	`Queries: 0 Referrals: 0`
	Information displayed:
	• Number of Queries and Referrals of the specified zone.
	• Each hostname currently committed under the specified zone
	• Number of Queries and Referrals for each hostname under the zone.

config dns zones <zonename> create-authority	Creates an authority record for the specified zone. Each zone can have up to five authority records and should have a minimum of two. Valid authority records require a fully qualified authority name (<authorityname>). Authority names cannot exceed 255 characters. Syntax: `config dns zones <zonename> create-authority <authorityname> ip <ip address>` where: **zonename** is the name of the zone for which you wish to create an authority record. **authorityname** is the name (hostname) of the host you wish to designate as an authority for the specified zone. **ip address** is the IP address of the host you wish to designate as an authority for the specified zone.

Config DNS Zones Commands

Command	Description
config dns zones <zonename> authority-ttl ***NOTE:*** *If all authority records are deleted under a specified zone, the authority TTL is reset to the default of 7200 seconds (two hours).*	Specifies the Time to Live (TTL) for authority records configured under the specified zone. Syntax: `config dns zones <zonename> authority-ttl <number>` where: **zonename** is the name of the zone whose authority records you wish to assign a Time to Live. **number** is the number of seconds assigned for TTL.
delete authority	Deletes the specified authority record for the specified zone. Syntax: `config dns zones <zonename> delete-authority <authority name> ip <ipaddress>` where: **zonename** is the name of the zone from which you wish to delete an authority record. **authority** name is the name of the authority record you wish to delete. **ip address** is the IP address of the host you wish to designate as an authority for the specified zone.
config dns zones <zonename> hostnames	Moves to the hostnames level.

config dns zones <zonename> hostnames info	Displays all hostnames under the specified zone.
	
	Syntax:
	`config dns zones <zonename> hostnames info`
	where:
	zonename is the name of the zone whose hostnames you wish to view.
	Information displayed:
	`Host: host1.com`
	`Method: wrr TTL: 60 Return Authoritative: Yes`

Config DNS Zones Commands

Command	Description

config dns zones <zonename> hostnames stats	Displays statistics information of all hosts configured under the specified zone. Each hostname with its corresponding number of resolutions is displayed.
	Syntax:
	`config dns zones <zonename> hostnames stats`
	where:
	zonename is the name of the zone whose hosts' statistics you wish to view.
	Information displayed:
	`Host: host1.com`
	`Queries: 0 Referrals: 0`
	
	`Host: host2.com`
	`Queries: 0 Referrals: 0`
	Queries - Total number of queries received under this host.
	Referrals - Total number of times that a particular host has been returned as the answer to a query.

config dns zones <zonename> hostnames create <atypehostname> ***NOTE:*** *When entering the hostname, do not include the zonename or the dot between the host and zone name. These are appended automatically. (Host and zonenames together may not exceed 255 characters.)*	Creates a host under the specified zone. Up to 512 hosts may be created. Syntax: `config dns zones <zonename> hostnames create <atypehostname>` where: **zonename** is the name of the zone under which you wish to create a new host. **atypehostname** is the name of the host you wish to create. The wildcard (*) and null (@) symbols can be substituted as a valid hostname. A wildcard (*) can be substituted for a hostname. If a request is made for an unconfigured hostname within a zone, all of the VIPs associated with the * hostname are returned (except any hostnames configured with the @ symbol). The @ symbol represents the null hostname in a zone. It permits the zonename to be substituted as a hostname. If a request is made to resolve just the zone, as if it were a host, the VIPs associated with the @ hostname are returned.

Config DNS Zones Commands

Command	Description
config dns zones <zonename> hostnames delete <atypehostname>	Deletes the specified host under the specified zone. All VIPs configured under the specified host are deleted as well. Syntax: `config dns zones <zonename> hostnames delete <atypehostname>` where: **zonename** is the name of the zone under which you wish to delete a host. **atypehostname** is the name of the host you wish to delete. The wildcard (*) and null (@) symbols can be substituted as a valid host name.
config dns zones <zonename> hostnames rename <atypehostname> new <atypehostname>	Renames the specified host under the specified zone. Syntax: `config dns zones <zonename> hostnames rename <hostname> new <hostname>` where: **zonename** is the name of the zone under which you wish to rename a host. **atypehostname** (1) is the current name of the host you wish to rename. The wildcard (*) and null (@) symbols can be substituted as a valid host name.

Config DNS Zones Commands

Command	Description
config dns zones <zonename> hostnames <hostname> info	Displays the specified host's configuration information. Syntax: `config dns zones <zonename> hostnames <hostname> info` where: **zonename** is the name of the zone of the host whose configuration information you wish to view. **hostname** is the name of the host whose configuration information you wish to view. • Fully qualified hostname (hostname.zonename) • Load balancing method (Weighted Round Robin, Weighted Random, Least Number of Connections, Average Response time, CPU utilization, or Flash.) • TTL (Time to Live) value • Authority (yes/no) • Maximum Additional Responses (Maximum allowed is 15). • Multiple VIP standby (enabled/disabled) • Site Services that are under this host.

stats	Displays the statistics information for the specified host in the specified zone.
	Syntax:
	`config dns zones <zonename> hostnames <hostname> stats`
	where:
	zonename is the name of the zone of the host whose statistics you wish to view.
	hostname is the name of the host whose statistics you wish to view.
	Information displayed:
	`Host: host1.com`
	`Queries: 0 Referrals: 0`

Config DNS Zones Commands

Command	Description
ttl	Configures the Time to Live (TTL) value, in seconds, for the specified zone/host. TTL is expressed an integer greater than or equal to zero and less than or equal to 65,535. Syntax: `config dns zones <zonename> hostnames <hostname> ttl <number>` where: **zonename** is the name of the zone of the host for which you wish to set the TTL. **hostname** is the name of the host for which you wish to set the TTL. **number** is the desired TTL value expressed in seconds.
method	Designates which of five available load balancing methods is to be used by the DNS server for this host. Syntax: `config dns zones <zonename> hostnames <hostname> method <lbmethod>` where: **zonename** is the name of the zone of the host for which you wish to specify the load balancing method. **hostname** is the name of the host for which you wish to specify the load balancing method. **lbmethod** is the acronym of the desired load balancing method (see below). **wrr** - Weighted Round Robin **wr** - Weighted Random **conn** - Least Number of Connections **avgresp** - Average Response Time **cpu** - CPU Utilization **flash** - Flash method

Config DNS Zones Commands

Command	Description
authority	If enabled, designates this 7190 as authoritative for the specified host. Default: enabled. Syntax: `config dns zones <zonename> hostnames <hostname> authority [enable|disable]` where: **`zonename`** is the name of the zone in which the host is located for which this 7190 is to be authoritative. **`hostname`** is the name of the host for which this 7190 is to be authoritative.
add-rec-responses <addrecrespval>	Sets the maximum number of additional A records that can be returned in a DNS response. The value ranges from 0 to 15. Syntax: `config dns zones <zonename> hostnames <hostname> add-rec-responses <addrecrespval>`
multi-vip-standby enable	When multi-VIP standby is enabled, VIPs that are marked as "NOT IN USE" and "NOT FAILED" are included in a multi-VIP response (if the number of additional VIPs in the response has not been met). The number of responses displayed are set with the **`add-rec-response`** command. Multi-VIP standby is disabled by default. Syntax: `config dns zones <zonename> hostnames <hostname> multi-vip-standby enable`
disable	Disables multi-VIP standby, if enabled.
config dns zones <zonename> hostnames <hostname> siteservices	Moves to the siteservices command level.
info	Displays information of all site services for this hostname.
stats	Displays statistical information of all site services.

Config DNS Zones Commands

Command	Description
map <site servicename>	Maps the combination of an agent and a service or an ISV name and service with the specified hostname. **siteservicename** = agentname:vip:port or **siteservicename** = isvname:vip:port
unmap <site servicename>	Removes the mapping of a service to this hostname.
config dns zones <zonename> hostnames <hostname> siteservices <siteservicename>	Moves to the siteservicename command level.
info	Displays information of the mapped service for this hostname specified by <siteservicename>.
stats	Displays statistical information of this site service.
enable	Enables this site service mapped for <hostname>. All services are enabled by default.
disable	Disables this site service mapped for <hostname>. This service is no longer available for resolutions for <hostname>.
standby	Configures the site service to be in standby mode. Standby services become enabled when enabled services are not available anymore.
weight	Sets or changes the weight of a site service for <hostname>. Services with higher weight are favored to services with lower weights. Weights can range between 1 and 255. Default = 1.
factor	Sets or changes the threshold for a site service based on the load balancing method (CPU/AVGRESP/LEAST CONN). Factor ranges between 1 and 255. Default value = 10.

Config DNS Zones Commands

Config DNS Flash Commands

Command	Description
config dns flash	Moves to the flash command level.

config dns flash info	Displays flash configuration information.
	For example:
	
	`Flash Information:`
	`  Flash State: Disabled  Aliasing: Disabled`
	`  Polling Interval: 10  Number of Polls: 100`
	`  Max Broadcast Delay: 500 Drop Misses: 3`
	
	Aliasing: With multiple 7190s, Flash responses can pass through a firewall because of the aliasing of source IPs.
	Polling Interval: How frequently Flash Peers are polled to determine the network latency
	Number of Polls: The number of Flash Peer polls to be used in calculating the average network latency between Flash Peers. The more polls, the slower the 7190 reacts to bursts of network congestion; but it is also slower to recover from long periods of congestion.
	Max Broadcast Delay: The maximum amount of time that a DNS response can be delayed to compensate for network latency between Flash Peers. If exceeded, may become out of sync with other peers.
	Drop Misses: The number of consecutive chances allowed for a response (to a poll message) before the peer 7190 is considered unavailable.

enable	Enables Flash load balancing.
disable ***NOTE:*** *If Flash is disabled, but the load balancing method selected is still 'flash', this results in an unweighted random (or 'straight' random) distribution.*	Disables Flash load balancing.

Config DNS Flash Commands

Command	Description
config dns flash max-delay	Sets the maximum time delayed before a response is returned, setting the maximum tolerated network latency between peer Flash agents. Default value is 5000ms. Range is 0 to 30,000ms. Syntax: `config dns flash max-delay <number>`
poll-interval	Specifies the interval, in seconds, at which a Flash agent polls its peer agents to determine the network latency to each peer. Default value is 10 seconds. Range is 1 to 255. Syntax: `config dns flash poll-interval <number>`
num-polls	Defines the number of data points involved in calculating the average network latency to a Flash agent. Each data point is the result of one completed poll. The default value is 100. Range is 10 to 255. Syntax: `config dns flash num-polls <number>`
drop-miss <number of misses>	Specifies the number of consecutive missed poll responses allowed before a flash peer is marked “unavailable”.
aliasing [enable|disable]	Enables or disables IP aliasing. The **`show dns flash info`** command displays whether aliasing is enabled or disabled.

Config DNS Flash Commands

Show Commands

Command	Description
show cli info	Displays the CLI configuration. Information displayed: • Number of concurrent Telnet sessions allowed • Root prompt • Number of login attempts allowed • More (‘paging’ enabled/disabled) • Number of screenlines • System ID • CLI timeout (in seconds)

show sys info	Displays the 7190’s system information.
	For example:
	`System Id:`
	`MAC Address: 0:90:27:73:f0:e4`
	`IP Address: 10.1.10.227`
	`Netmask: 255.255.0.0`
	`Broadcast: 10.1.255.255`
	`Default Route: 10.1.1.1`
	`Nameservers: mysite-ex.com`
	`10.1.1.10`

date	Displays the system date.
ntp info	Displays the names/IP address of NTP servers configured for this 7190.

Show Commands

Command	Description
show sys snmp info	Displays the status of the SNMP-related variables. Information displayed: • SNMP (enabled/disabled) • Auto-topology (enabled/disabled) • SNMP agent port • SysName • SysContact • SysLocation
logs display	Displays the contents of the specified log file. Syntax: `show sys logs display <all|dns|ntp|system|monitor|stats>` where: **`all`** - displays all log messages **`dns`** - displays DNS activity and health monitor information on this 7190. **`ntp`** - displays NTP messages **`system`** - displays system messages **`monitor`** - displays monitoring messages **`stats`** - displays statistical information
show sys logs display-old	Displays the contents of the old log file. Syntax: `show sys logs display-old <log>` where: **`log`** is the designation for the log file whose contents you wish to view. Log file designations: • system • dns • ntp • all • stats

Command	Description
software info	Displays information regarding installed software. The list of installed software images includes: • Image index number of each installed version • Product description of each installed version • Version number of each installed version • Patch number, if any • Build numbers of each installed version • An indicator (‘Running’) of which version is currently running.
ssh info	Displays the current status of SSH enable or disable. If the status was just changed, it reflects the changed status that is pending for the reboot.
wizard info	Displays whether Quick Start Wizard is enabled or disabled. To enable or disable Wizard, use **`config sys wizard [enable|disable]`**.
show dns info	Displays DNS information pertaining to this 7190. Information displayed: • Status, primary / secondary • If secondary, the primary IP • Logging enabled / disabled

Show Commands

Command	Description

flash info	Displays flash information, including whether flash *aliasing* is on or off. See **`config dns flash spoof`** for information.
	
	`Flash Information:`
	`  Flash State: Disabled  Aliasing: Disabled`
	`  Polling Interval:  10  Number of Polls: 100`
	`  Max Broadcast Delay: 500 Drop Misses:  3`
	
	Aliasing: With multiple 7190s, Flash responses can pass through a firewall because of the aliasing of source IPs.
	Polling Interval: How frequently Flash Peers are polled to determine the network latency
	Number of Polls: The number of Flash Peer polls to be used in calculating the average network latency between Flash Peers. The more polls, the slower the 7190 reacts to bursts of network congestion; but it is also slower to recover from long periods of congestion.
	Max Broadcast Delay: The maximum amount of time that a DNS response can be delayed to compensate for network latency between Flash Peers. If exceeded, may become out of sync with other peers.
	Drop Misses: The number of consecutive chances allowed for a response (to a poll message) before the peer 7190 is considered unavailable.

Command	Description
show dns stats	Displays DNS statistical information: • **Queries** - Total number of DNS queries received. • **Referrals -** Total number of times that a particular service or group of services have been returned as the answer to a query. • **Unknown Zones -** Total number of queries received for hosts in zones that the 7190 is authoritative for, but do not exist in the configuration. • **Malformed -** Total number of received queries that violated the syntax rules for a proper DNS request packet. • **Queries/Sec** - Total number of queries per second. • **Refused -** Total number of received queries for information that is refused for policy reasons. • **Unknown Hosts -** Total number of queries received for hosts in zones that the 7190 is authoritative for, but do not exist in the configuration. • **Unsupported -** Total number of queries for unsupported DNS response types. For example requests for MX (mail) records would return Unsupported. • **Avg Queries/Sec** - Average number of queries per second.
info all	Displays the DNS state (Enabled/Disabled, Primary/Secondary), and all 7190 information for all configured Agents, Services, ISV Groups, Zones, Hosts, and Flash Information.
stats all	Displays the DNS Statistics (see **`stats`** command for definitions), and all 7190 information for all configured Agents, Services, ISV Groups, Zones, Hosts, and Flash Information.
show dns status	If the 7190 is a primary, it displays the secondary 7190s to which it is currently connected. If the 7190 is a secondary, it displays the connection status to its primary.

Show Commands

Command	Description

show dns zones info	Displays the names of all committed zones of this 7190, and the Time-to-Live (TTL) of their authority records.
	For example:
	`Zone: mysite-ex.com`
	`Authority Records TTL: 86400`

stats	Displays the statistics on all zones committed under this 7190. Zone names are displayed followed by the number of resolutions for each.
	For example:
	`Zone: mysite-ex.com`
	`Queries: 0 Referrals: 0`

show dns zones <zonename> info	Displays displays all the host names committed under the specified zone.
	For example
	`Zone: mysite-ex.com`
	`Authority Records TTL: 86400`
	`Hostnames:`
	`host1.com`

stats	Displays the number of queries and referrals per hostname for the specified zone.
	For example
	`Zone: mysite-ex.com`
	`Queries: 0 Referrals: 0`
	`Host: host1.com`
	`Queries: 0 Referrals: 0`

show dns zones <zonename> hostnames info	Displays all hostnames under the specified zone.
	Syntax:
	`show dns zones <zonename> hostnames info`
	Information displayed:
	`Host: host1.com`
	`Method: wrr TTL: 60 Return Authoritative: Yes`

Show Commands

Command	Description

stats	Displays all the hostnames and their number of queries and referrals.
	Syntax:
	`show dns zones <zonename> hostnames stats`
	Information displayed:
	`Host: host1.com`
	`Queries: 0 Referrals: 0`

show dns zones <zonename> hostnames <hostname> info	Displays committed hostname, the load balancing method, the TTL, the authority of the specified host, and any site services. Information displayed:
	`Host: host1.com`
	`Method: wrr TTL: 60 Return Authoritative: Yes`
	`Site Services:`

stats	Displays the statistics of the specified hostname. Syntax: `show dns zones <zonename> hostnames <hostname> stats` Information displayed: • Hostname • Number of Queries received. • Number of Referrals (the number of times that a service has been returned as the answer to a query).

show dns agents info	Displays information for all configured agents. Information displayed:
	`Agent: load1`
	`State:Enabled Metrics Interval:30 Metrics Timeout:15`
	`Agent IP: 10.1.2.8 Agent Port: 1999`
	`Primary Flash Src: Not Defined Primary Flash Port: 0`
	`Backup Flash Src: Not Defined Backup Flash Port: 0`
	`Agent: load2`
	`State:Enabled Metrics Interval:30 Metrics Timeout:15`
	`Agent IP: 10.2.2.2 Agent Port: 1999`
	`Primary Flash Src: 10.2.2.2 Primary Flash Port: 200`
	`Backup Flash Src: Not Defined Backup Flash Port: 0`

Command	Description

stats	Displays statistics for all committed agents.
	Syntax:
	`show dns agents stats`
	Information displayed:
	`Agent: load1 (Version 45.0.0.0)`
	`State: Connected CPU Util: 5% Connections/Sec: 0`
	`Agent: load2 (Version Unknown)`
	`State: Connected CPU Util: 0% Connections/Sec: 0`

metrics	Displays metrics information for each committed agent. For information, see **`show dns agents stats`** command.

Show Commands

Command	Description
show dns agents metrics <agentname> port <port #>	Displays metrics for the specified unconfigured agent. If specified agent does not exist or if a connection cannot be established, an error message appears. Syntax: `show dns agents metrics <agent ip> port <port#>` Information displayed: • Agent IP • Agent Port • Agent Version Number • Agent State • CPU utilization • Average Connections per Second If Agent State is "OK," then each VIP associated with this agent is displayed with the service info. Service info includes: • VIP • Port • Type • Number of Servers • Average Response Time • Load Balancing Method • Validation of LB Method

Command	Description

show dns agents <agentname> info	Displays information about the specified agent.
	Information displayed:
	`Agent: load1`
	`State:Enabled Metrics Interval:30 Metrics Timeout:15`
	`Agent IP: 10.1.2.8 Agent Port: 1999`
	`Primary Flash Src: Not Defined Primary Flash Port: 0`
	`Backup Flash Src: Not Defined Backup Flash Port: 0`
	Metrics Interval: How frequently the load balancer is to update the 7190 with its service metrics information.
	Metrics Timeout: How long beyond the expected reporting time that the 7190 waits for service metrics information from a local balancer.

stats	Displays statistical information (agent name, state, service information, etc.) for the specified agent.
	Syntax:
	`show dns agents <agentname> stats`
	Information displayed:
	`Agent: load2 (Version Unknown)`
	`State: Disconnected CPU Util: 0%`
	`Connections/Sec: 0`
	`Service: 10.5.5.5:90 (0 Servers, No Connection)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`

Show Commands

Command	Description

show dns agents <agentname> metrics	Displays metrics information for a single specified agent.
	Syntax:
	`show dns agents <agentname> metrics`
	Information displayed is:
	• Agentname
	• Agent Version Number
	• Agent State
	• CPU Utilization
	• Average Connections per Second
	• All services configured for this agent.
	For example:
	`Agent: load2 (Version Unknown)`
	`State: Connected CPU Util:0% Connections/Sec:0`
	`Service: 10.5.5.5:90 (0 Servers)`
	`Referrals: 0 Flash Referrals: 0`
	`Response Time: 0 Connections/Sec: 0`

services info	Displays information of all services configured under this agent.
services stats	Displays statistical information of all services for the specified agent.
services <servicename> info	Displays configuration information of the specified service name.
services <servicename> stats	Displays statistical information of a configured service.

Show Commands

Command	Description
show dns agents <agentname> metrics <ip address> port <port#>	Displays metrics for the specified unconfigured agent. If specified agent does not exist or if a connection cannot be established, an error message appears. Syntax: `show dns agents <agentname> metrics <ip address> port <port#>` Information displayed: • Agent IP • Agent Port • Agent Version Number • Agent State • CPU utilization • Average Connections per Second If Agent State is "OK," then each VIP associated with this agent is displayed with the service information. Service information includes: • VIP • Port • Type • Number of Servers • Average Response Time • Load Balancing Method • Validation of LB Method
show dns isvgroups	Moves you to the isvgroups command level.

Show Commands

Command	Description

show dns isvgroups info	Displays the list of all ISV groups, their states, flash information, probe information and the services configured for them.
	For example:
	`ISV Group: isv2`
	`State: Enabled Probe Interval:30 Probe Timeout:15`
	`Primary Flash Src:10.1.1.1 Primary Flash Port:2000`
	`Backup Flash Src: 10.1.1.2 Backup Flash Port: 2000`
	`ISV Group: isv3`
	`State:Enabled Probe Interval:30 Probe Timeout:15`
	`Primary Flash Src: Not Defined Primary Flash Port:0`
	`Backup Flash Src: Not Defined Backup Flash Port:0`
	Probe Interval: How frequently the services in an ISV group are polled for availability.
	Probe Timeout: How long to wait for a response to an ISV service availability poll.

show dns isvgroups <isvname> info	Displays information of all services committed for the ISV. For example:
	`ISV Group: isv5`
	`State: Enabled Probe Interval:30 Probe Timeout:15`
	`Primary Flash Src: 10.1.1.1 Primary Flash Port: 2000`
	`Backup Flash Src:Not Defined Backup Flash Port: 0`
	`Services:`
	`10.4.4.4:80`

stats	Displays all statistical information within the specified ISV Group, such as Services and their respective statistics. For example:
	`Service: 10.4.4.4:80`
	`Referrals: 0 Flash Referrals: 0 Response Time:`

show dns isvgroups <isvname> services info	Displays information for the specific ISV Group: state (enabled/disabled), flash information, probe information, and any configured services.
show dns isvgroups <isvname> services stats	Displays service statistics for any services configured for this specific ISV Group.

Show Commands

Command	Description
show dns isvgroups <isvname> services <svcname> info	Displays service information for the specific service under the specific ISV Group.
stats	Displays service statistics for the specific service under the specific ISV Group. For example: Service IP and Port, Number of Referrals and Flash Referrals, and Response Time.

Show Commands

7 SNMP Support

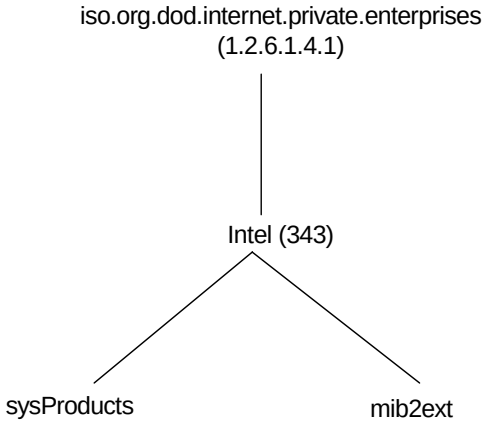
The Intel® NetStructure™ 7190 Multi-Site Traffic Director has a fully compliant, embedded SNMP agent that supports SNMPv1 and SNMPv2 requests. In addition to standard MIB-II, Intel private enterprise MIBs provide the capabilities to monitor the performance and health of the 7190.

Standards Compliance

The 7190 SNMP agent is bilingual and can support both SNMPv1 and SNMPv2c requests. All traps are sent in SNMPv2c format. Intel private enterprise MIB files are compliant with SMIv2 as specified in RFC 1902. The SNMP agent supports Management Information Base -II (MIB-II) as specified in RFC 1213, but allows SET operations only on the SYSTEM and SNMP groups.

Intel® MIB Tree

The following illustrates the top level of the MIB tree.



MIB Tree (top level)

All Intel enterprise MIBs and MIB objects are defined under the mib2ext branch of the Intel® tree. All `sysObjectIds` that identify Intel products are defined under the `directors` branch of the MIB tree.

Supported MIBs

Management Information Base-II (MIB-II)

Intel Enterprise MIBs:

```
ceo-header.my
multisite-mib.my
```

Nortel Auto-topology MIBs:

```
s5emt103.my
s5roo114.my
s5tcs112.my
synro167.my
```

Where to find MIB Files

Electronic copies of the MIB files used by the 7190 are shipped with the product on CD-ROM and are available from Intel's web site at http://www.intel.com/support/ipivot/software.htm. Nortel Auto-topology MIB files are available from Nortel and at http://www.intel.com/support/ipivot/software.htm. A password is required for access.

The standard SNMP traps, `coldStart`, `warmStart`, `authenticationfailure`, `linkUp` and `linkDown` are supported.

ceo-header.my

`ceo-header.my` contains the objects that define the top-level branches of the MIB tree.

multisite-mib.my

`multisite-mib.my` has the following structure:

```
agentMetricsTable
   agentMetricsEntry
      agentIpAddress
      agentVersion
      agentState
      agentCpuUtil
      agentCps
serviceMetricsTable
   serviceMetricsEntry
      serviceVip
      sevicePort
      serviceType
      serviceAvgRespTime
      serviceActiveServers
msdConnState
siteNumber
```

```
isvTable
  isvEntry
    isvIndex
    isvVipAddr
    isvVipPort
    isvProbeType
    isvProbeState
    isvProbeProperties
siteTable
  siteEntry
    siteIndex
    siteName
```

Agent Metrics Group

Object	Description
agentMetricsTable	An agent runs in a load balancer (i.e., 7140 & 7170) which communicates with the Multi-Site. The agentMetricsTable conains load balancer performance data reported by the agent to the Multi-Site.
agentMetricsEntry	Each entry contains the last metrics information returned by a remote load balancer agent.
agentIpAddress	IP address of remote load balancer agent.
agentVersion	Version of remote load balancer agent.
agentState	Polling state of the remote load balancer agent. `noConnection`: A TCP connection cannot be established with remote load balancer agent `Fail`: No info was received in response to last poll `OK`: remote agent responded to last poll
agentCpuUtil	CPU usage (percentage amount) of remote load balancer agent.
agentCps	Connections per second of remote agent.

Agent Metrics Group

Service Metrics Group

Object	Description
serviceMetricsTable	An agent runs in a load balancer which communicates with the MSD 9000. The serviceMetricsTable contains load balancer performance data reported by the agent to the Multi-Site pertaining to service (VIP and port).
serviceMetricsEntry	Each entry contains the last metrics information returned by a remote load balancer agent for a service (i.e, VIP and port).
serviceVip	VIP of the service
servicePort	Port number of the service
serviceType	Type of the service
serviceAvgRespTime	Average response time (in milliseconds) of the service
serviceActiveServers	Number of active servers for the service

Service Metrics Group

ISV Metrics Group

Object	Description
isvTable	List of ISV entries. The number of entries is given by the value of the siteNumber.
isvEntry	An ISV entry containing VIP objects.
isvIndex	A unique value for each ISV. Its value ranges between 1 and the value of siteNumber.
isvVipAddr	IP address that is used for probing.

ISV Group

Object	Description
isvVipPort	Server TCP port number.
isvProbeType	ISV probe type can be Ping or TCP or HTTP. The Ping is an ICMP probe. The TCP Probe opens a TCP session, sends no data and resets the connection after receiving an appropriate response. The acceptable response is the TCP acknowledgment that a connection can be established. The HTTP probes have a user configurable URL. A connection is made to that URL, an HTTP get is performed, and the header results examines any of the 400 or 500 range error codes and update the status of the URL.
isvProbeState	The current state of the ISV probe: • noConnection (0) • noMetrics (1) • noServiceAvailable (2) • serviceAvailable (3)
isvProbeProperties	Lists URL and other information.

ISV Group

Site Group

Object	Description
siteNumber	The number of 7190 ISVs and agents, regardless of their current state, present on this system.
siteTable	List of agents and ISV entries. The number of entries is given by the value of siteNumber.
siteEntry	Site entry containing agent name or ISV name.
siteIndex	A unique value for each site, ranging between 1 and the value of the siteNumber
siteName	The agent name or ISV name.

Site Group

SNMP Traps

The following list summarizes the traps generated by the 7190. For details about a particular trap, please read the description of each MIB above, or read the documentation within the MIB file. Traps are generated by SNMPv2c

```
coldStart
authenticationFailure
linkUp
```

multisite-mib.my

```
agentStateChanged
shuttingDown
configurationChanged
connStateChanged
serviceAvailable
serviceFailed
isvProbePingAlert
isvProbePingNormal
isvProbeTcpNormal
isvProbeTcpAlert
isvProbeHttpUrlNormal
isvProbeHttpUrlAlert
```

Object	Description
msdConnState	Connection state of the 7190. A primary 7190 always has the state primary. A secondary 7190 can have the state connected, refused or retrying, indicating its connection state to its primary 7190.
shuttingDown	7190 is shutting down.
configurationChanged	7190 configuration has changed.
connStateChanged	The 7190 connection state has changed. A primary 7190 always has the state primary. A secondary 7190 can have the state Connected, Refused, or Retrying.
serviceAvailable	Standby or Active VIP is available.
serviceFailed	When a site fails, any available standby site becomes active.
isvProbePingNormal	VIP is responding to Ping, and the server is back to normal.
isvProbePingAlert	VIP is not responding to Ping.
isvProbeTcpNormal	VIP is responding to TCP Stack probe. Server TCP Stack back to normal.
isvProbeTcpAlert	VIP is not responding to TCP Stack probe.
isvProbeHttpUrlNormal	VIP is responding to HTTP probes.
isvProbeHttpUrlAlert	VIP is not responding to HTTP probes.

SNMP Traps

s5emt103.my, s5roo114.my, s5tcs112.my, synro167.my

These files are the Nortel Auto-topology MIB files. When auto-topology is enabled, the 7190 periodically broadcasts auto-topology packets, which include the following information:

- The IP address of the sender
- The segment ID used by the sender for this segment
- The MAC address of the sender
- The chassis type of the sender

- The backplane type of the sender, for the 7190 this is enetFastEnet (10).
- Local segment indication. This indicates whether the sender is on the same ethernet segment or across a bridge.
- The current state of the auto-topology packet's sender.

The 7190 listens for auto-topology packets from other nodes and uses these to maintain tables of information about the other nodes on the segment. Network management applications use SNMP to access such tables throughout the network to provide current topological information to the network administrator. The MIB tables contain the information list above plus the following

- The slot on which the packet was received. For the 7190 this is always "1."
- The port on which the packet was received. For the 7190 this is always "1."

Displaying SNMP Parameters

NOTE: *Ensure that the 7190's IP Filtering security mechanism allows IP access to SNMP, otherwise SNMP requests do not pass through the filter.*

In the CLI, use the following command to display all SNMP parameters:

```
show sys snmp info
```

Configuring Community Authen-tication & Security Parameters

The 7190 SNMP supports community-based authentication. Up to ten community strings can be configured for use by the 7190. Each community string can have read-only (ro) or read-write (rw) privilege, and can be configured for use by a specific IP address or all IP addresses. When the value any is used for `<ip address>`, the community string can be used by all IP addresses.

The following CLI commands are used to display and configure SNMP community strings.

```
config sys snmp community info
config sys snmp community create <string> ip <ip
address> rights [ro|rw]
config sys snmp community delete <string> ip <ip
address>
```

For example:

```
config sys snmp community create test ip
209.218.240.5 rights ro
```

This command creates the community string test with read-only privilege. SNMP read-only requests using community string test are accepted only from IP address 209.218.240.1.

By default the following community strings are defined:

```
public ro any
private rw any
```

Configuring Trap Parameters

Use the following CLI commands to display and configure SNMP trap parameters:

```
config sys snmp trap info
config sys snmp trap port <port>
config sys snmp trap create <ip address>
community <community>
config sys snmp trap delete <ip address>
community <community>
```

By default, the UDP port used for sending traps is 162. The trap port can be changed to a number between 5020 and 65535, or left at 162.

The 7190 SNMP can send trap notifications to up to ten configured trap receivers. Each IP address configured as a trap receiver is associated with a community string included in traps sent to that IP address. For example:

```
config sys snmp trap create 209.218.240.5
community NOC1
```

This command causes traps to be sent to IP address 209.218.240.5, and causes the 7190 SNMP agent to put the community string NOC1 in the trap.

Configuring Other SNMP Parameters

The following CLI commands are used to display and configure general SNMP parameters:

```
config sys snmp info
config sys snmp port <port>
config sys snmp sysContact <string>
config sys snmp sysName <string>
config sys snmp sysLocation <string>
config sys snmp auto-topology [enable|disable]
```

SNMP port is the UDP port used by the 7190 SNMP to listen for SNMP requests. By default, the SNMP port is 161. The SNMP port can be changed to a number between 5020 and 65535, or left at 161.

`sysContact`, `sysName` and `sysLocation` correspond to the MIB variables of the same name in MIB-II. `sysContact` is the name of the administrator of this 7190. By default, `sysContact` is null. `sysName` is the name of the 7190. By default, `sysName` contains the hostname of the 7190. `sysLocation` indicates where the 7190 is physically located. By default, `sysLocation` is null.

Support for Nortel Auto-topology protocol is enabled with `auto-topology`. By default, `auto-topology` is disabled. When enabled, the Auto-topology protocol automatically executes whenever SNMP runs.

Notes

8 Software Updates

Your Intel® NetStructure™ 7190 Multi-Site Traffic Director unit is shipped with the latest system software installed. After initial installation and setup, you may be eligible for, or choose to purchase a software version update. This chapter describes the update procedure.

Multiple Software Images

The 7190 provides sufficient local storage for at most five software images (though at any time, only one image is active and executing.) You can download and install new software images on the 7190 by using the CLI command **`config sys software install`**. (See the section titled, “Displaying and Selecting the New Image for Boot” for information on how to run alternate stored images.)

Software Image Media

Depending on the circumstances, you may receive your software update on a CD-ROM as part of a new software kit, or you may download it from an Intel software web site. In either case, the

distribution consists of a single large binary file of approximately 20 megabytes. The first step in software installation is to place this install image file on an ftp server accessible by the 7190.

NOTE: *Username commands are not valid in configuration files, i.e.,* **`save config`** *and* **`restore config`** *operations do not include username data.*

Saving Your Current Configuration

7190 configurations are by default preserved across major software updates. It is however recommended that you save your existing 7190 configuration while running your currently installed software. You can save your current configuration with the **`save`** command.

Downloading and Installing the Software

The process for downloading and installing the software is the same whether the image is a version update or patch. Once the install file is on an ftp server, you use the CLI to instruct the 7190 to download and install it. Although it is possible to install software while the 7190 is operating, it is recommended that a backup 7190 be configured before installation to minimize your downtime. If no backup is available, it is best to perform installation at off-peak times. To install the image, use the command **`config sys software install`**.

NOTE: *You need the ftp server's hostname, a user name, password, and the image's filename.*

When you have these items, execute **`config sys software install`** from the 7190 CLI. The following is an example of the syntax for ftp downloads.

```
Config sys software install ftp://
FTPURL<imagename> user <myftpuser> password
<myftppw>
```

Status information appears as the installation progresses. If the install status information indicates that the installation failed due to incorrect URL, user name, or password information, verify this data and reenter the command with the appropriate corrections.

Rebooting with the New Image and Verifying Installation

NOTE: *If any errors occurred during installation,* **`show sys software`** *may display the image as installed, however it is not safe to use. Use* **`config sys software delete`** *to delete the image and repeat the installation before continuing. If the problem persists, contact Intel Technical Support.*

When the image has been downloaded and installed, it can be verified by typing **`show sys software info`**. For example, after downloading and installing an update, **`show sys software info`** may display the following:

Index	Product	Version	Patch	Build
1	7190	3.0	1.0	D1
2	7190	3.1	0.0	D12 (running)

This indicates that the image at index 1 has been installed and is ready for service, and the image at index 2 is running. To activate the new image, type **`config sys software boot 1`**. The 7190 reboots under the new image. This command can also be used to revert to the previous version.

Restoring Your Previous Configuration

After the 7190 reboots and comes up under the new image, you can restore your previous configuration with the **`restore`** command.

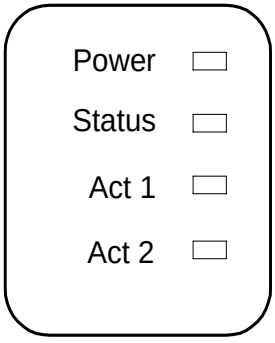
Notes

A Diagnostics

This section describes the available diagnostic information and in-field diagnostics procedures for the 7190.

Diagnostic LEDs

The front panel's LEDs provide information generated by the boot-time power-on-self-test (POST) and application startup sequences. There are four LEDs on the front panel, as shown.



Diagnostic LEDs

Power Indication

The front panel Power LED connects directly to the unit's power supply. If the Power LED is not illuminated, power is not connected to the unit, or the unit's power supply has failed.

Boot-time LED Diagnostics

The front panel's Status, Act 1 and Act 2 LEDs display the transition through a sequence of codes at boot time indicating the product's progress through the boot process. If the boot process aborts, terminates, or halts before the product is online and functional, the state of the LEDs can help in diagnosing the problem. The following table describes the startup sequence and conditions.

Status	Act 1	Act 2	Condition	Console Message
Off	Off	Off	BIOS boot failed	
On	Off	Off	OS boot process failed	Starting OS….
Off	On	Off	OS boot stage 1 failed	OS Phase 1….
On	On	Off	OS boot stage 2 failed	OS Phase 2….
Off	Off	On	OS boot stage 3 failed	OS Phase 3….
On	Off	On	Application never started up	
Off	On	On	Application restart stage 1 failed	
On	On	On	Application restart stage 2 failed	

Boot-Time LED Diagnostics

After restart completes, the Status LED begins to blink and LED activity begins as described in the next section, "Runtime LED Diagnostics."

Runtime LED Diagnostics

Runtime Activity

At runtime, the LEDs provide information about system activity as described below.

Status LED

- Blinks on and off quickly when operating normally.
- Continuous on or off indicates troubled (hung) system.

Activity LEDs

The following table describes the runtime behavior of the Status and Activity LEDs (Act 1, Act 2)

Runtime Errors

Status	Act 1	Act 2	Condition
1 sec on, 1 sec off	Off	Off	DNS Server is Running
1 sec on, 1 sec off	Solid	Off	1000 – 3500 DNS Queries/sec
1 sec on, 1 sec off	Solid	Solid	> 3500 DNS Queries/sec
Solid	Solid	Solid	DNS Server is Down
Off	Off	Flash	NIC Failure
Flash	Flash	Flash	Health Montoring Failure (each LED lights in sequence)

Runtime Errors

At runtime, the 7190's health-monitoring processes indicate critical error conditions by turning off the Status LED and flashing error patterns on the two Activity LEDs.

System Log

The system log contains diagnostic messages from various software modules of the 7190. The system log memory is of limited size (512K bytes) and wraps around when the allocated space has been filled up.

Log Message Format

There are five components to each log message in this file.

```
(Date) (Time)   (Hostname) (Module) (Text)
Aug 2  14:28:03  mstd1     DNSD:   Starting..
```

The Date and Time fields indicates when the message was logged.

The Hostname field indicates the name of the 7190 which owns the log.

The Process field indicates which software module wrote the message to the log. The possible values for the Module field are DNSD, WDOG, NCA, BACKEND, DNS_STATS, and DBPRD.

The Text field contains the text of the message being logged.

Displaying Log Messages

The following command is used to display the contents of the system log.

```
config sys logs display
[system|dns|ntp|stats|all]
```

Specify **system** to display the log messages from the BACKEND module only. Specify **dns** to display messages from the DNSD, NCA, WDOG and DBPRD modules. Specify **stats** to display messages from the DNS_STATS module. Specify **all** to display all messages in the log.

The DNSD module can be configured to log every dns request and response it processed. To enable this feature, use the following command.

```
config dns log [enable|disable]
```

Descriptions of the six modules and the messages they generate follow.

DNSD: The DNS Server Daemon process

This process logs a message when it is started and when reading in the configuration. Severe or fatal errors are logged with a preceding "ERROR". Others messages may be logged with or without "WARNING" based on the nature of the event.

Example:

This message is logged when the dns server is started.

```
Aug 2 14:28:03 madagascar DNSD: Starting 7190
DNS Server
```

This message is logged when the dns server reads the configuration file at boot time.

```
Aug 2 14:28:03 madagascar DNSD: Reading in
configuration...
Aug 2 14:28:04 madagascar DNSD: Finished
processing cfg -> Host recs: 165; Agent recs:
2; Authority recs 10
```

WDOG: The Watch Dog process

This process is in charge of monitoring all background processes. Watchdog starts all the background process before the user is logged in. If any of the above processes die, watch dog restarts them. This information is logged to the system log.

Example:

This message is logged when the watch dog monitor starts running.

```
Aug 2 14:28:04 madagascar WDOG: Info: Watchdog
Monitor started (201)
```

These messages are logged when a process terminates and restarts Watch Dog also restarts all dependent process with the process that was restarted.

```
Aug 2 14:28:05 madagascar WDOG: Info: Process
801 terminated. /usr/local/geo/bin/nca
Aug 2 14:28:05 madagascar WDOG: Info: Process
10297 started. /usr/local/geo/bin/nca
```

NCA (Network Configuration Application)

This process is in charge of connecting to and talking to the agents resident on the 7140/7170 or 7180 devices. It also connects to and talks to the dns server and the backed process. It is the NCA that updates configuration information of the dns server every time user types a commit command.

Some of the messages that are logged by the NCA are:

```
Aug 2 12:13:27 madagascar NCA: NCA has
started.
```

This message is displayed when NCA tries to establish connection to an agent on the specified port.

```
Aug 2 12:13:27 madagascar NCA: Connection
established to address 192.168.16.3 on port
1999.
```

When connection to an agent fails the following message is displayed.

```
Aug 3 01:27:23 fox NCA: >>> Error: Connection
to address 192.168.16.27 on port 2037 has
failed.
```

Other major errors include the following:

This message is displayed when a socket connection failed to establish. The “code” is an internal error code.

```
Aug 3 01:27:23 fox NCA: >>> Error: Failed to
establish 192.168.16.3 on port 2000, code: 61.
```

This message is displayed when NCA process could not allocate memory for its internal use.

```
Aug 3 01:27:23 fox NCA: >>> Error: could not
allocate memory. Bytes requested: 1024.
```

Log messages are also generated when switching between primary and secondary mode, and when getting new configuration from the primary 7190.

BACKEND Process

This process is the bridge between the front end CLI command handler and the DNS server. All information goes through backend.

Backend writes to the log only on two occasions.

When the process is started / restarted

```
Aug 2 12:13:32 madagascar WDOG: 7190 Backend
started
```

```
Aug 2 12:13:33 madagascar BACKEND: Reading in
configuration...
Aug 2 12:13:33 madagascar BACKEND: ***Backend
is ready for the user*
```

When there is an error reading the configuration file, these errors are logged specifying the error and the line where it occurred.

DNS_STATS Daemon

This daemon is in charge of collecting statistics from the dns server. Every 15 minutes DNS_STATS module logs the number of queries that were made since the last log write.

Example:

```
Aug 3 01:26:05 fox DNS_STATS: Average number
of queries per second since last log: 7246
```

DBRPD: Database Print Server Daemon

This is a database print server daemon that is used to obtain statistical information directly from the DNS server. The module logs a message in daemon log when the process is started.

Notes

B Cleaning the Dust Filter

The Intel® NetStructure™ 7195 Multi-Site Traffic Director has a dust filter element mounted behind the front grille and in front of the dual intake fans. This filter is washable and should be cleaned every six months at a minimum. If you use your 7190 in an abnormally dusty environment, clean the filter more often. You need not interrupt 7190 operation to perform the following cleaning procedure.

To clean the filter:

- Remove the two Phillips screws that secure the metal grille on the left side of the 7190's front panel. Remove the grille to expose the foam filter element.
- Remove the filter element from its recess. It is recommended that you replace the grille and its screws while the filter element is being cleaned.
- Wash the filter in warm water and set aside to dry.

Allow the filter to dry thoroughly before reinstalling in the 7190.

- When the filter element is dry, remove the 7190's front grille and replace the filter in its recess, assuring that its entire perimeter is behind the metal lip of the recess.
- Reinstall the grille with its two Phillips screws.

Notes

C Regulatory Information

Taiwan Class A EMI Statement

警告使用者 ：
這是甲類的資訊產品， 在居住的環境中使用時，
可能會造成射頻干擾， 在這種情況下，使用者會
被要求採取某些適當的對策。

VCCI Statement

Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Internal access to Intel equipment is intended only for qualified service personnel.

FCC Part 15 Compliance Statement

This product has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning this equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Change the direction of the radio or TV antenna.

- To the extent possible, relocate the radio, TV, or other receiver away from the product.
- Plug the product into a different electrical outlet so that the product and the receiver are on different branch circuits.

If these suggestions don't help, consult your dealer or an experienced radio/TV repair technician for more suggestions.

NOTE: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION: If you make any modification to the equipment not expressly approved by Intel, you could void your authority to operate the equipment.

Canada Compliance Statement (Industry Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

CE Compliance Statement

This NetStructure™ 7190 Multi-Site Traffic Director complies with the EU Directive, 89/336/EEC, using the EMC standards EN55022 (Class A) and EN50082-1. This product also complies with the EU Directive, 73/23/EEC, using the safety standard EN60950.

CISPR 22 Statement

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI Class A (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Australia

WARNING

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.

- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.

Do not attempt to modify or use the supplied AC power cord if it is not the exact type required.

Ensure that the system is disconnected from its power source and from all telecommunications links, networks, or modem lines whenever the chassis cover is to be removed. Do not operate the system with the cover removed.

AVERTISSEMENT

Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit être:

- Propre et dépourvu de poussière en suspension (sauf la poussière normale).
- Bien aéré et loin des sources de chaleur, y compris du soleil direct.
- A l'abri des chocs et des sources de ibrations.
- Isolé de forts champs magnétiques géenérés par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques il est recomandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage.
- Muni d'une prise murale correctement mise à la terre.

Ne pas utiliser ni modifier le câble d'alimentation C. A. fourni, s'il ne correspond pas exactement au type requis.

Assurez vous que le système soit débranché de son alimentation ainsi que de toutes les liaisons de télécomunication, des réseaux, et des lignes de modem avant d'enlever le capot. Ne pas utiliser le système quand le capot est enlevé.

WARNUNG

Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der entwickelt. Der Standort sollte:

- sauber und staubfrei sein (Hausstaub ausgenommen);
- gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);
- keinen Erschütterungen ausgesetzt sein;
- keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- mit einer geerdeten Wechselstromsteckdose ausgerüstet sein.

Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht um genau den erforderlichen Typ handelt.

Das System darf weder an eine Stromquelle angeschlossen sein noch eine Verbindung mit einer Telekommunikationseinrichtung, einem Netzwerk oder einer Modem-Leitung haben, wenn die Gehäuseabdeckung entfernt wird. Nehmen Sie das System nicht ohne die Abdeckung in Betrieb.

AVVERTENZA

Il sistema è progettato per funzionare in un ambiente di lavoro tipico. Scegliere una postazione che sia:

- Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell’ambiente).
- Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.
- Al riparo da urti e lontana da fonti divibrazione.
- Isolata dai forti campi magnetici prodotti da dispositivi elettrici.

- In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem.
- Dotata di una presa a muro correttamente installata.

Non modificare o utilizzare il cavo di alimentazione in c. a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto.

Prima di rimuovere il coperchio del telaio, assicurarsi che il sistema sia scollegato dall'alimentazione, da tutti i collegamenti di comunicazione, reti o linee di modem. Non avviare il sistema senza aver prima messo a posto il coperchio.

ADVERTENCIAS

El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar:

- Limpio y libre de partículas en suspensión (salvo el polvo normal)
- Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.
- Alejado de fuentes de vibración.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas.
- Previsto de una toma de tierra correctamente instalada.

No intente modificar ni usar el cable de alimentación de corriente alterna, si no se corresponde exactamente con el tipo requerido.

Asegúrese de que cada vez que se quite la cubierta del chasis, el sistema haya sido desconectado de la red de alimentación y de todos lo enlaces de telecomunicaciones, de red y de líneas de módem. No ponga en funcionamiento el sistema mientras la cubierta esté quitada

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.

15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einerqualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sint beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanscluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

Notes

D Terms and Conditions and Software License

Intel Corporation

END USER TERMS AND CONDITIONS OF SALE AND SOFTWARE LICENSE

IF THE PRODUCT IS PURCHASED DIRECTLY FROM INTEL AND UNLESS SUCH PARTIES HAVE ENTERED INTO A BILATERALLY EXECUTED AGREEMENT, WHICH EXPRESSLY TAKES PRECEDENCE, THE TERMS AND CONDITIONS STATED HEREIN WILL APPLY.

IF THE PRODUCT WAS PURCHASED FROM AN INTEL CHANNEL PARTNER, THEN ONLY SECTIONS 13-23 APPLY TO THE END USER.

1. **Entire Agreement:** These terms and conditions ("Agreement") for the sale of hardware and license of software, which includes the associated documentation shipped with the hardware and software ("Product"), constitute the complete and exclusive statement of all the terms of the Agreement between Intel Corporation, ("Intel") and the purchaser using the Product for its ordinary internal operation of its business and not for resale ("End User") and supersedes all prior understandings, writings, proposals, representations or communications, oral or written, relating to the subject matter hereof and unless subsequent different, contradictory or additional terms and conditions are agreed to in a writing signed by authorized representatives of both parties. In no event shall this Agreement be deemed an acceptance by Intel of any terms and conditions included with End User's purchase order or similar End User document. Intel's performance hereunder is expressly conditioned on End User's assent to this Agreement.

2. **Orders:** End User may purchase Product by submitting a valid purchase order ("Order") to Intel at the corporate address stated herein. Orders are subject to Intel's written acceptance ("Order Acceptance"). Order Acceptance is based in part to approval of credit by Intel to End User as set forth in the "Credit Terms" Section of this Agreement.
3. **Term and Termination Date:** This Agreement shall be effective on the date of the Order Acceptance and continue in effect until terminated by either party upon thirty (30) days advance written notice unless terminated earlier for breach.
4. **Price:** The price to be paid by End User shall be that stated on the Order as accepted on the Order Acceptance. All prices are in U.S. dollars.
5. **Credit Terms:** Credit terms are made at Intel's sole discretion by analysis of End User's current and historical financial and credit information, bank and trade references, payment practices, etc. End User agrees to provide such information to Intel upon request. Intel reserves the right to refuse payment terms if, in Intel's sole discretion, such terms would create an unreasonable credit risk. In that event, deliveries will be available only on a C.O.D., cash-in-advance, or irrevocable letter of credit basis.
6. **Delivery:** Subject to the Section below entitled "Leasing/Renting," if applicable, Products shall be shipped Ex Works (1990 Incoterms), Intel's shipping dock. End User is responsible for payment of all costs relating to transportation, delivery, and insurance, which shall be pre-paid by Intel and added to the invoice, unless otherwise agreed to on the Order Acceptance. Title and risk of loss shall pass to End User upon delivery to the first common carrier except that shipments to destinations outside of the United States are subject to the "Security Interest and Reservation of Title" Section of this Agreement.
7. **Security Interest And Reservation Of Title:** End User hereby grants to Intel a purchase money security interest covering each shipment of Products made hereunder (and any proceeds thereof) in the amount of Intel's invoice for such shipment until Intel receives payment in full. (A purchase money security interest only applies to Products purchased by End User and the proceeds from the sale of such Products by End User.) End User agrees to sign and execute any and all documents as required by Intel to perfect such security interest. For Products shipped to destinations outside of the United States, Intel reserves title in such Products until End User pays Intel in full for such Products, at which time title in such Products shall pass to End User (except that in the case of software, only title to the media shall pass).
8. **Cancellation:** Orders cancelled within five (5) days of scheduled shipment may be subject to a ten percent (10%) cancellation charge.
9. **Payment Terms:** Payment in full is due thirty (30) days after date of the invoice. Intel may charge End User interest on any delinquent balance at the lesser of eighteen percent (18%) per year or the maximum amount permitted by law. Intel may refuse shipment to End User if End User is delinquent in making payments to Intel.

10. **Taxes and Duties:** End User is responsible for all taxes imposed in connection with sale to End User of Products or services which Intel may incur under this Agreement (except taxes imposed on Intel's income) including but not limited to all import duties, customs fees, levies or imposts, and all sales, use, value added, gross receipts or other taxes of any nature and any penalties, interest and collection or withholding costs associated with any of the foregoing items. All such amounts are in addition to other amounts payable hereunder and this obligation shall survive termination or expiration of this Agreement. If applicable law requires End User to withhold any income taxes levied by the authorities of Canada on payments to be made pursuant to this Agreement ("Withholding Tax"), End User shall take advantage of the reduced Withholding Tax provided for by the Canada-United States tax treaty then in force and shall be entitled to deduct such Withholding Tax from the payments due to Intel hereunder. End User is further responsible for obtaining import licenses and preparing and submitting all required documentation in connection with importing Products including obtaining and providing to Intel International Import Certificates and other supporting documentation required by Intel in order to apply for United States export licenses.

11. **Leasing/Renting:** Subject to the provisions of this Section, End User may request to have Products delivered to it under a leasing/renting arrangement between End User and a lessor/owner ("Lessor"). Intel's obligations to accept any Order from Lessor and to deliver Product pursuant to such Order from Lessor are limited to the following circumstances:

    11. 1. The Lessor is Intel who will retain title to the Product and accept lease or rent payments; or

    11. 2. Any Lessor, other than Intel Order, provided that:

        11. 2. 1. The Order indicates on its face that Lessor is ordering the Product identified in the Order on behalf of End User;

        ii. The Order indicates on its face that it is in accordance with, and subject to,

        iii. The terms and conditions of this Agreement; and

        iv. Intel's credit department has approved the Lessor.

    With respect to any Order issued by any Lessor, other than Intel, subject to any specific provisions found in a bilaterally-executed agreement between Intel and Lessor, Lessor will be considered End User's agent for the purpose of ordering Product and making payment and the rights and obligations of End User and Intel identified in this Agreement shall remain except for the following:

    (1). Title to Product delivered pursuant to such Order shall be presumed vested in Lessor;

    (2). The license accompanying the Product shall apply to Lessor; and

    (3). Notwithstanding anything to the contrary in the license accompanying the Product, Lessor may transfer such title and license rights to End User under a leasing arrangement.

12. **Returns:** No Product may be returned except under warranty for repair or due to shipment error by Intel.

13. **Software License:** Intel grants End User a non-exclusive, non-transferable (except as set forth in this Section) non-exclusive, restricted right to use the Intel software as incorporated in or supplied with the Intel hardware and solely in connection with the operation of the Product for End User's own internal business purposes. End User understands that Intel may update the Intel Product from time to time and such changes shall be subject to this license grant. End User may transfer the license to use the Intel software only in connection with a sale or transfer of the Product and as included with the Product and not on a standalone basis, provided the transferee agrees to be bound by the terms and condition of this Agreement. Intel and its suppliers retain all title to, and, except as expressly licensed herein, all rights to the software, all copies thereof, and all related documentation and materials. End User may not use, copy, modify, create derivative works of, distribute, sell, assign, pledge, sublicense, lease, loan, rent, timeshare, deliver or otherwise transfer the Intel software, nor permit any other party to do any of the foregoing.

14. **No Modifications To Product:** Product is shipped in its complete form and structure; no modifications are needed. End User shall not, nor permit any other party to modify, reverse engineer, reverse compile, or disassemble any part of Product, including any attempt to translate the Intel software, derive or attempt to derive the software source code or any part thereof. Any modification or attempt described herein will void the warranties of this Agreement.

15. **Limited Software Warranty:** Intel warrants to the first End User purchaser that the media containing the software is free from defects for a period of ninety (90) days from date of shipment. End User assumes responsibility for the selection of the appropriate network or computing equipment, software, and associated materials. Intel makes no warranty or representation that the software will work in combination with any third-party network or computing equipment or software, that the operation of the software will be uninterrupted or error free, or that all defects in the software will be corrected. No updates are provided under this Agreement. No warranties for third party software are provided by this warranty.

16. **Limited Hardware Warranty:** Intel warrants to the original owner that the product delivered in this package will be free from material defects in material and workmanship for one (1) year following the latter of: (i) the date of purchase only if you register by returning the registration card as indicted thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed.

    THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

    This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may

replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA): Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling the non-toll free numbers below:

North America only: (858) 391-1900
Other locations: Return the product to the place of purchase.

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

Limitation of Liability and Remedies: INTEL SHALL HAVE NO LIABLILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THE PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCED NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Europe only

Intel warrants to the original owner that the product delivered in this package will be free from defects in material and workmanship for one (1) year following the later of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

English	+44 1793 404900
French	+44 1793 404988
German	+44 1793 404777
Italian	+44 1793 404141

Returning a Defective Product (RMA): Return the product to the place of purchase for a refund or replacement.

Limitation of Liablility and Remedies: INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

This limited Hardware Warranty shall be governed by and construed in accordance with the Laws of England and Wales. The courts of England shall have exclusive jurisdiction regarding any claim brought under this warranty.

17. **Export Law Regulations:**

    17. 1. Applicable Laws. End User acknowledges that all Products, spares, documentation or other materials (collectively "Product") are subject to applicable import and export regulations of the United States and of the countries in which End User transacts business, specifically including U.S. Export Administration Act and Export Administration Regulations. This Agreement is also specifically subject to U.S. Department of Commerce regulations relating to restrictive trade practices or boycotts and the Foreign Corrupt Practices Act. In no event shall Intel be bound by any terms and conditions which contravene applicable laws. End User shall comply with all laws and regulations applicable to the Product. Without limiting the generality of the foregoing, End User agrees that it shall not export, re-export, transfer or divert any of the Product or the direct product thereof to any restricted place or party in accordance with U.S. export regulations.

    17. 2. License Exceptions. End User acknowledges that certain of the Product are exported under U.S. Export Administration Regulation license exceptions which prohibit transfer, export or re-export to military end-users or for military uses or for use with regard to nuclear, chemical or biological weapons activity including projects, design, production or stockpiling such weapons. End User is responsible for compliance with all such license exceptions.

    17. 3. Responsibility for Export Licensing. Intel agrees to use commercially reasonable steps to obtain, at Intel's expense, all documentation required by the United States Office of Export Administration and/or other authorities to permit the exportation of Product to End User. End User shall take all actions and provide all information reasonably requested by Intel in order for Intel to obtain such export licenses. Intel shall have no liability or obligation to End User if the responsible government authorities decline to issue any such export licenses. ALL ORDERS ISSUED PURSUANT TO THIS AGREEMENT ARE SUBJECT TO THE OBTAINING SAID LICENSES.

    17. 4. Import Certificates. End User is responsible for obtaining and providing to Intel International Import Certificates and other supporting documentation required by Intel in order to apply for United States export licenses.

    17. 5. Encrypted Products. Products containing encryption may require additional restrictions. Sale of these specific items may require End User's written consent to comply with any such additional restrictions prior to shipment of the Products.

    17. 6. Letter of Compliance. Intel may require End User to execute a Letter of Compliance, as it deems reasonable to meet the requirements of applicable export regulations.

18. **United States Government Legend:** The software and documentation is commercial in nature and developed solely at private expense. The software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

19. **Copyrights; Trade Secrets:** End User acknowledges and agrees that the structure, sequence and organization of the software (including but not limited to any images, photographs, animations, video, audio, music, and text) are the valuable trade secrets of Intel and its suppliers. End User agrees to hold such trade secrets in confidence. End User further acknowledges and agrees that ownership of, and Intel and its suppliers hold title to, the Product, its copyrights and patents and all subsequent copies thereof regardless of the form or media. End User may not remove from the Product, or alter, any of the trademarks, trade names, logos, patent or copyright notices or making, or add any other notices or marking to the Product.
20. **Governing Law:** The rights and obligations of the parties hereunder shall be construed in accordance with, and all disputes hereunder shall be governed by, the laws of the State of California excluding conflict of law rules and excluding the United Nations Convention on Contracts for the International Sale of Goods. The Superior Court of San Diego County, California and/or the United States District Court for the Southern District of California shall have jurisdiction and venue over all disputes between the parties.
21. **Attorney's Fees And Costs:** In any legal action to enforce this Agreement, or arising out of the sale or licensing of Products hereunder, the prevailing party shall be awarded all court costs and reasonable attorney's fees incurred.
22. **Force Majeure:** Intel shall not be liable to End User for any alleged loss or damage resulting from the delivery of the Products being delayed by acts of End User, acts of civil or military authority, governmental priorities, earthquake, fire, flood, epidemic, quarantine, energy crisis, strike, labor trouble, war, riot, accident, shortage, delays in transportation, or any other causes beyond Intel's reasonable control.
23. **Excusable Delay:** Neither party shall be liable to the other for any alleged loss or a damage resulting from a delay in performance resulting from a cause beyond the reasonable control of the party whose performance is delayed.
24. **Choice Of Language.** The original of this Agreement is in English and End User waives any right to have it written in any other language.
25. **Notices.** Any notice regarding non-performance, breach, termination, or renewal required or permitted to be given under this Agreement shall be given in writing and shall be hand delivered or deposited, postage prepaid, registered or certified mail, in the United States or other country's mail, or sent by express delivery, addressed to End User or Intel, as the case may be, at the addresses stated on the Order or at such other address as shall be given by either one to the other in writing. All other notices may be sent by regular mail or facsimile. All notices shall be deemed given and received on the earlier of actual delivery or three (3) days from the date of postmark.
26. **No Assignment:** End User may not transfer or assign the Product or this Agreement to another party without the prior written consent of Intel.

Glossary

This section defines terms and acronyms used throughout the *Intel® NetStructure™ 7190 Multi-Site Traffic Director User Guide*.

Agent Refers to a load balancer (7140, 7170, or 7180), specifically to the fulfillment agent on a load balancer, which communicates service availability and metric information related to the VIPs brokered by the load balancer to a 7190. All VIPs associated with an agent share a common Flash Source.

Broker Better known as a load balancer (7140, 7170, or 7180). The term is often used as an adjective to describe a site containing load balancers, e.g., a “brokered” site.

CPU Utilization of Load Balancer Algorithm that monitors load balancer workload and directs clients to the site with the lowest workload.

DHCP Dynamic Host Configuration Protocol. This protocol allows servers to dynamically assign IP addresses to nodes (workstations) on the fly.

DNS Domain Name Server. A nechanism used in the Internet for translating the names of host computers into addresses.

Flash Response Mode	A solution to DNS site balancing based on network latency. Rather than attempt to actual measure network latency to a client DNS server, Flash DNS broadcasts separate responses simultaneously from each of the balanced sites. The response from the site with the least network latency to the client DNS server arrives first to be used. All other responses are discarded by the client DNS server as part of normal DNS protocol.
Flash Peer	Broadcaster of a Flash DNS answer.
Flash Source	A Flash Source is the Flash Peer that is responsible for referring VIPs associated with an Agent or Pseudo-Agent when Flash DNS site balancing is used. The Flash Source generally must be on the same network as the Agent/Pseudo-Agent or at least behind the same router. When Flash DNS support is enabled on a load balancer, both the Flash Source and Agent have the same address (the online outside IP address of the load balancer).
Global Sync	The process of automatically transferring (copying) the primary 7190 configuration to a secondary 7190.
HTTP	Hypertext Transfer Protocol: the protocol used between a web browser and a server to request a document and transfer its contents.
HTTPS	HTTP exchanged over an SSL-encrypted session.
IP	Internet Protocol
IP Address	A unique identifier for a node on an IP network. Expressed in “dotted decimal” notation. For example: 10.0.0.1.
IP Service	A network-accessible, IP-accessible Application Protocol. For example: HTTP, FTP, and the like. For administration purposes of the Intel Netstructure products, services are identified by Virtual IP:Port.
ISV	Intelligent Site Verification. Intelligent Site Verification is used to determine the availability of a third-party load balancer site. Methods of verification include a site ping, TCP connect, and HTTP probe.
ITM (Internet Traffic Manager)	Intel® NetStructure™ 7140 and 7170 Traffic Director products, used for load balancing.
Least Connections	This algorithm sends requests to the site with the lowest number of connections. Least connections offers more effective management for long sessions, such as FTP.

Load Balancer	Intel® 7140, 7170 or 7180
Load Balancing	The distribution of processing and communications activity across a computer network so that no single device is overwhelmed. Load balancing is particularly important for networks on which it is difficult to predict the volume of requests likely to be issued to a server. Busy Web sites typically employ two or more Web servers in load balancing roles.
MIB	Management Information Base. A repository of characteristics and parameters managed in a network device, such as a NIC, hub, switch, or router.
NAT	Network Address Translation. This function is usually performed by firewalls to hide internal network addresses from the outside world. This technique is often used when a large pool of users on a local network are sharing a small pool IP addresses that are valid to the outside world. Firewalls performing NAT are unable to determine the proper translation for packets originating from outside that they have no knowledge of an internal packet being sent to.
NIC	Network Interface Card. The attachment that connects a device to a network by executing the code needed by the connected device to share a cable or some other media with other stations.
Port	The service port associated with a service.
Primary and Secondary 7190s	The initial 7190 configuration is performed on a *primary* 7190, and is then automatically transferred (copied) to any 7190s designated as *secondaries*. This process is called Global Sync.
Peer	A secondary 7190 that has been committed.
Service	A service is an application protocol that is offered on a network. The device where the service is running is identified by an IP address. A port is used to identify the protocol at the designated IP address. Services contain an IP address and a port. For example, `10.54.67.6:80` describes a service consisting of a server's HTTP application listening on port 80.
Server Response Time	This algorithm directs requests to the site with the fastest aggregate (i.e., across all servers) response time for the requested VIP. The 7190 knows about all of the VIPs for a particular site and knows which one is performing best at that moment.
SNMP	Simple Network Management Protocol.

Aliasing	The act of trying to appear as a legitimate packet from a trusted or expected source even though the packet actually originated at some unknown source.
SSL (Secure Socket Layer)	Protocol developed by Netscape for encrypted transmission over TCP/IP networks, setting up a secure end-to-end link.
TCP/IP	Transmission Control Protocol (TCP) utilizing IP as the base transport.
TTL	DNS Time To Live.
UDP/IP	User Datagram Protocol (UDP) utilizing the IP as the base transport. It is an unreliable, but fast transport mechanism. It is used by DNS.
VIP	A virtual IP address of a site. It may be the actual IP address of a non-brokered server. At a brokered site a VIP is used to group resources. The VIP address is mapped to the resources IP addresses. A Broker balances VIP network traffic across its resources.
Weighted Random	This algorithm resolves IP address randomly, rather than serially, while weighting works as in Weighted Round Robin. The benefit of this algorithm is that it is more effective at normalizing, or leveling, load than Weighted Round Robin.
Weighted Round Robin	This algorithm is an enhancement of legacy Round Robin DNS, under which IP addresses are returned serially from the server's list of addresses. The differences between Round Robin DNS and Weighted Round Robin are site status awareness and weighting. Weighting allows site operators to skew loading on a percentage basis. For example, Site A might be weighted to receive 12.5% of the traffic, site B 25 % and site C 62.5%.

Support Services

Intel® offers a range of support services for your new product. You can learn about the options available for your area by visiting the Intel® support web site at http://www.intel.com/network/services and choosing your geography.

Worldwide Access to Technical Support

Intel has technical support centers worldwide. Technicians who speak the local languages staff many of the centers. Visit our web site at http://support.intel.com/.

North America only

For support, call **(800) 838-7136** or **(916) 377-7000**.

Japan only

For support, call **+81-298-47-0800**.

Other areas

For support in other countries, use the following table to dial the toll-free support number. Using the table, locate the country from which you are calling, dial the access number, await the dial tone and then dial the listed 800 number.

Country	Dialing Information
Australia	Dial 1-800-881-011, await dial tone, dial 800-838-7136
China [3]	Dial 10811, await dial tone, dial 800-838-7136
Hong Kong	Dial 800-1111, await dial tone, dial 800-838-7136
India [5]	Dial 000-117, await dial tone, dial 800-838-7136

Country	Dialing Information
Indonesia [2]	Dial 001-801-10, await dial tone, dial 800-838-7136
Korea [1]	Dial 0-911, await dial tone, dial 800-838-7136
Malaysia [4]	Dial 800-0011, await dial tone, dial 800-838-7136
New Zealand	Dial 000-911, await dial tone, dial 800-838-7136
Singapore	Dial 800-0111-111, await dial tone, dial 800-838-7136
Sri Lanka	Dial 430-430, await dial tone, dial 800-838-7136
Taiwan [1]	Dial 0080-10288-0, await dial tone, dial 800-838-7136
Thailand [5]	Dial 0019-991-1111, await dial tone, dial 800-838-7136
Austria [1 4]	Dial 022-903-011, await dial tone, dial 800-838-7136
Belgium [1]	Dial 0-800-100-10, await dial tone, dial 800-838-7136
Denmark	Dial 8001-0010, await dial tone, dial 800-838-7136
Finland [1]	Dial 9800-100-10, await dial tone, dial 800-838-7136
France (Includes Andorra)	Dial 19-0011, await dial tone, dial 800-838-7136
Germany	Dial 0130-0010, await dial tone, dial 800-838-7136
Italy (Includes Vatican City) [1]	Dial 172-1011, await dial tone, dial 800-838-7136
Netherlands [1]	Dial 06-022-9111, await dial tone, dial 800-838-7136
Norway	Dial 800-190-11, await dial tone, dial 800-838-7136
Poland [1 3]	Dial 0-0-800-111-1111, await dial tone, dial 800-838-7136
Portugal [3]	Dial 05017-1-288, await dial tone, dial 800-838-7136
Russia [1 2 3]	Dial 755-5042, await dial tone, dial 800-838-7136
Spain	Dial 900-99-00-11, await dial tone, dial 800-838-7136
Sweden	Dial 020-795-611, await dial tone, dial 800-838-7136

Country	Dialing Information
Switzerland [1]	Dial 0-800-550011, await dial tone, dial 800-838-7136
United Kingdom (Mercury) [3]	Dial 0500-89-0011, await dial tone, dial 800-838-7136
United Kingdom (BT) [3]	Dial 0800-89-0011, await dial tone, dial 800-838-7136
RSA (South Africa)	Dial 0-800-99-0123, await dial tone, dial 800-838-7136
Philippines	Dial 105-11, await dial tone, dial 800-838-7136
Vietnam	Dial 12010288, await dial tone, dial 800-838-7136
Pakistan	Dial 0080001001, await dial tone, dial 800-838-7136

Notes:

1	Public phones require coin or deposit
2	Use phones allowing international access
3	May not be available from every phone
4	Public phones require local phone payment through the call duration
5	Not available from public phones

Notes

Index

Symbols

A

B

C

T

W

Z

Notes